UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE: APPLE IDEVICE ADDRESS BOOK LITIGATION	Case No.: 13-CV-00453-JST **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL** Also consolidating: No. 12-CV-1515-JST No. 12-CV-1529-JST No. 12-CV-6550-JST

Plaintiffs Haig Arabian, Alan Beuershasen, Giuli Biondi, Lauren Carter, Steve Dean, Stephanie Dennis-Cooley, Jason Green, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali Mandaywala, Claire Moses, Judy Paul, Maria Pirozzi, Theda Sandiford and Greg Varner, individually and on behalf of all others similarly situated, allege as follows based on personal knowledge of their acts and, otherwise, upon information and belief based on investigation of counsel. This Complaint consolidates four separate cases under a single Complaint, as ordered by the Court. Not all Plaintiffs bring all causes of action herein, as different Plaintiffs are represented by separate counsel. The identity of the Plaintiffs bringing each cause of action is indicated in the heading of each respective cause of action.

INTRODUCTION

1. Apple Inc. ("Apple") designs and manufactures three popular wireless mobile devices: the iPhone, the iPod touch and the iPad (collectively, the "iDevices"). Since Apple launched the first iPhone in 2008, iDevices have propelled the company's popularity and revenue, and have been a game changer for Apple and the mobile device industry in general.

2. An integral aspect of the iDevices' popularity (and their design) is the ready availability of mobile software applications ("apps") for these devices. Apps are available exclusively from an Apple-controlled "App Store," even apps developed by third parties.

3. Since 2008, Apple's promotions of iDevices have touted that the App Store (and access to App Store add-on iDevice apps) is included with every iDevice purchased, that Apple facilitates, controls and polices the development and sales channel for add-on iDevice apps, that protection of iDevice user privacy was paramount, that iDevices were not susceptible to and that the App Store would not provide apps containing malicious, hidden, unforeseen or privacy-invading features, and that iDevice security features (such as "sandboxing") nevertheless protected and secured iDevices and the iDevice owners' materials and information from malicious or ill-conceived apps by compartmentalizing apps and their data-sets from one another.

4. Apple has publicly claimed that it is well aware of the content and features of each add-on iDevice app that it has made available to and deployed on consumers' iDevices via the App Store. For years Apple has touted that purported awareness to market its iDevices and associated App Store apps (and cultivate perceptions about product security and quality) and has asserted that it has "raised the bar for consumers' rich mobile experience beyond what [Apple] or anyone else ever imagined both in scale and quality."

5. In a mid-2009 open letter to the Federal Communications Commission that Apple has kept posted on its public website (the "FCC Letter," available at http://www.apple.com/hotnews/apple-answers-fcc-questions/), Apple described the App Store as "an innovative business model," "a frictionless distribution network," and "the world's largest wireless applications store," and stated that "to [in part] protect consumer privacy," it "reviews every application" and subjects each to a "comprehensive review [and rejection] process" (including for "privacy issues") before putting an app on the App Store, and confirmed that Apple, in its sole discretion, decides whether an app does or does not make it to the App Store (and, subsequently, to consumers' iDevices). Apple further emphasized its policy against apps that transfer iDevice users' "contacts databases" from their iDevices to developers' servers, noting in

the FCC Letter its rejection of competitor Google's *Google Voice* app because "the iPhone user's entire Contacts database is transferred to Google's servers, and we [Apple] have yet to obtain any assurances from Google that this data will only be used in appropriate ways."[1]

6. Apple emphasized these competitive selling points (particularly to contrast competitors' offerings) repeatedly in extensive marketing and advertising campaigns, public relations campaigns, press releases, product launches, seminars, executive interviews, speeches and keynote addresses (and in Apple's FCC Letter and its lawsuit against Amazon.com over the App Store™ trademark) and they were significant factual enticements to – and part of the basis of the bargain with – each Plaintiff and other consumers to purchase iDevices and to accept additional add-on apps for their purchased iDevices from Apple.

7. Nevertheless, unbeknownst to Plaintiffs, and to other consumers of iDevices, apps built by certain app companies, including Defendants Chillingo Ltd.., Foodspotting, Inc., Foursquare Labs, Inc., *Gowalla* Incorporated, Hipster, Inc., *Instagram*, Inc., Kik Interactive, Inc., Path, Inc., Rovio Entertainment, Ltd., Twitter, Inc., Yelp! Inc., ZeptoLab UK Limited, and Facebook (for any period during which it controlled, managed or operated *Gowalla* or its iDevice app) (collectively, the "App Defendants"), and available through the App Store have been secretly uploading and disseminating user personal information (including private mobile address books) without user knowledge or consent. Despite its claims to the contrary, Apple failed to safeguard the iDevices and has failed to warn consumers of the danger associated with downloading apps from the App Store.

8. Plaintiffs bring this class action on behalf of themselves and (i) other purchasers of iDevices during the defined Class Period who downloaded apps from App Store (the "iDevice Class"); (ii) others who received the App Defendants' apps from Apple during the Class Period (the "Malware Subclass"); and (iii) other iDevice owners whose valuable private mobile address books were publicly disclosed or obtained by the App Defendants and whose iDevices were

[1] Apple's FCC Letter does not disclose that the *Google Voice* app had been on the App Store for roughly four months before Apple pulled it.

intermeddled with during the Class Period as a result of undisclosed features hidden in Defendants' apps, but known to Apple (the "Address Book Subclass").

9. Plaintiffs purchased their iDevices with the expectation that Apple designed these devices to protect their privacy and would have not purchased the iDevice and/or would have paid less for them had they known Apple designed iDevices in such a way as to make these devices vulnerable to unauthorized access by third-parties. Despite Apple's representations to the contrary, App Defendants and Apple deployed (through Apple's App Store) apps containing computer contaminants and spyware capable of taking control of Plaintiffs' iDevices in violation of internal, industry, contractual and legal standards, and the undisclosed but known susceptibility of iDevices to hidden, malicious functions like those inherent in Defendants' iDevice apps identified herein.

10. Plaintiffs purchased their iDevices and received one or more of Defendants' identified Apps[2] from the App Store.

11. This Court has previously sustained Plaintiff Maria Pirozzi's claims that Apple (1) violated the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq*.; (2) violated the False and Misleading Advertising Law ("FAL"), Cal. Bus. & Prof. Code §17500, *et seq*.); (3) violated the Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code. §1750 *et seq*.; and (4) made negligent misrepresentations to the Class.

JURISDICTION AND VENUE

12. This Court has original jurisdiction of this action under the Class Action Fairness Act of 2005. The amount-in-controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, there are 100 or more class members, and there is minimal diversity because certain members of the class are citizens of a different state than any Defendant as required by 28 U.S.C. § 1332(d)(2).

[2] Apple is a joint developer of each app. As described below, each app incorporates substantial Apple-created content and is "digitally signed" (i.e., configured for iDevice activation and compatibility) by Apple.

13. This Court also has original jurisdiction of this action under 28 U.S.C. § 1331 (federal question) because Plaintiffs seek recovery for Defendants' violations of the Computer Fraud & Abuse Act ("CFAA"), 18 U.S.C. § 1030(g), the Racketeer Influenced & Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1961, *et seq.*, and the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2520, *et seq*. This Court also has supplemental subject matter jurisdiction over Plaintiffs' related state law claims under 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendants. Each Defendant regularly conducts business in this judicial district and this action arose, at least in part, out of each Defendant's business in this judicial district. Each App Defendant (defined below) has done substantial business in California, with Apple, and with Plaintiffs directly related to the iDevice apps at issue in this case, including appointing Apple as their agent to market and deploy the apps to Plaintiffs' iDevices. The following Defendants are also headquartered within this federal judicial district: Apple Inc., Electronic Arts, Inc., Facebook, Inc., Foodspotting, Inc., Hipster, Inc., Instagram, Inc., Path, Inc., Twitter, Inc., and Yelp! Inc. Thus, all Defendants have sufficient minimum contacts with the United States, California, and this judicial district so that they are amenable to service of process, including under California's long-arm statute and the nationwide reach of the RICO statutes, 18 U.S.C. § 1965(b), and so that requiring them to respond to this action would not violate due process. Additionally, the Court previously determined in its transfer order (ECF No. 217) that all Defendants are subject to personal jurisdiction in the Northern District of California.

15. Venue is proper in this District under 28 U.S.C. § 1391(b) because each Defendants' improper conduct alleged in this Complaint occurred in, was directed from, and/or emanated from, in whole or in part, this judicial district. Additionally, the Court previously determined in its transfer order (ECF No. 217) that venue of this action is proper for all Defendants in the Northern District of California.

THE PARTIES[3]

Plaintiffs

16. Plaintiff Haig Arabian is a resident of Los Angeles County, California. Arabian downloaded and used the *Instagram* App on his iDevice during the Class Period (as defined below). When Arabian purchased his iPhone, he expected his contacts not to be accessible to other apps. He chose to upgrade from his Blackberry to the iPhone because he wanted a smartphone that had apps, he perceived the iPhone to be a secure alternative to the Blackberry, and relied on Apple's reputation for safety. Arabian purchased his iPhone with the expectation that he would be able to download and utilize apps available through the App Store without compromising the safety of his personal and private information. If Arabian knew that the apps would be able to potentially steal his private contacts, he would not have paid as much for the iPhone, or would not have purchased the iPhone. At no time did Apple warn Arabian that his iPhone may be vulnerable to unauthorized access by third-parties.

17. Plaintiff Alan Beuershasen resides in Austin, Texas. During the Class Period, Plaintiff Beuershasen owned and regularly used an iPhone with the following iDevice apps: *Twitter, Gowalla, Foursquare* and *Angry Birds Classic*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

18. Plaintiff Giuli Biondi resided in Austin, Texas. During the Class Period, Plaintiff Biondi owned and regularly used an iPhone with the following iDevice apps: *Instagram, Twitter, Yelp!* and *Cut the Rope*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

[3] Plaintiffs Beuershasen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul, Sandiford and Varner brought the case *Opperman, et al. v. Path, Inc., et al.*, No. 13-CV-00453 (W.D. Tex. Mar. 12, 2012) (transferred to N.D. Cal. Jan. 31, 2013) against all Defendants named in this consolidated action. Plaintiff Lauren Carter brought the case *Hernandez v. Path, Inc.*, No. 12-CV-01515 (N.D. Cal. Mar. 26, 2012) against Defendant Path, Inc. Plaintiff Maria Pirozzi brought the case *Pirozzi v. Apple Inc.*, No. 12-CV-01529 (N.D. Cal. Mar. 27, 2012) against defendant Apple. Plaintiff Haig Arabian brought the case *Gutierrez v. Instagram, Inc.*, No. 12-CV-06550 (N.D. Cal., Dec. 27, 2012) against Defendant *Instagram*, Inc.

19. Plaintiff Lauren Carter is a resident of Los Angeles County, California. Carter downloaded and used the *Path* App on her iPhone during the Class Period (as defined below). Carter saw in-store advertisements prior to purchasing her iPhone. She chose to upgrade from her Blackberry to the iPhone because she wanted a smartphone that had apps, she perceived the iPhone to be a secure alternative to the Blackberry, and relied on Apple's reputation for safety. Carter purchased her iPhone with the expectation that she would be able to download and utilize apps available through the App Store without compromising the safety of her personal and private information. The apps were an essential part of the device for Carter. Carter keeps private contact information of her family and friends on her iPhone. When Carter purchased her iPhone she expected her contacts not to be accessible to other apps. If Carter knew that the apps would be able to potentially steal her private contacts she would not have downloaded the apps and would not have paid as much for the iPhone, or would not have purchased the iPhone. At no time did Apple warn Carter that her iPhone may be vulnerable to unauthorized access by third-parties.

20. Plaintiff Steve Dean resided in Austin, Texas. During the Class Period, Plaintiff Dean owned and regularly used an iPhone with the following iDevice apps: *Twitter, Gowalla* and *Angry Birds Classic*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

21. Plaintiff Stephanie Dennis-Cooley resides in Virginia. During the Class Period, Plaintiff Dennis-Cooley owned and regularly used an iPhone and an iPad with following Apps: *Twitter, Kik Messenger, Path* and *Instagram*. Each identified app was placed, deployed and used on Plaintiff's iDevices before February 2012.

22. Plaintiff Jason Green resides in Fayetteville, Arkansas. During the Class Period, Plaintiff Green owned and regularly used an iPhone with the following iDevice apps: *Instagram, Twitter, Kik Messenger, Path, Angry Birds Classic* and *Cut the Rope*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

23. Plaintiff Claire Hodgins resides in Austin, Texas. During the Class Period, Plaintiff Hodgins owned and regularly used an iPhone with the following Apps: *Twitter, Yelp!, Angry Birds*

Classic and *Cut the Rope*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

24. Plaintiff Gentry Hoffman resides in Austin, Texas. During the Class Period, Plaintiff Hoffman owned and regularly used an iPhone with the following Apps: *Twitter, Instagram, Foursquare* and *Yelp!*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012. Plaintiff Hoffman has purchased multiple iPhones from 2008 onward. In particular, he purchased the iPhone 3g in or around 2008, the iPhone 3gs in or around 2009, the iPhone 4 in 2010, the iPhone 4s in 2011. He waited in line and purchased these iDevices at the Apple Store in Austin. Prior to making these purchases, he reviewed Apple's website and saw numerous in store, print and television ads concerning the products. He also watched numerous live blogs and web announcements in which the new iPhone products were discussed and launched. These blogs and web announcements include specifically those led by Steve Jobs and referenced herein. He continues to review these launches and announcements on line and intends to so again when the next launch is scheduled. Plaintiff Hoffman relied upon the information on Apple's website, ads, blogs and announcements in making his purchase. Based on the foregoing, Plaintiff Hoffman believed that the iPhone was a closed system, that Apple protected him from malware and malicious apps, and that his address book information was private and could not be taken without his consent. Had he known this to be false, Plaintiff Hoffman would not have purchased the above devices nor accepted apps from the App Store that uploaded or disclosed his mobile address book without his consent. Plaintiff Hoffman overpaid for the devices as a consequence of the above.

25. Plaintiff Rachelle King resides in Austin, Texas. During the Class Period, Plaintiff King owned and regularly used multiple iPhones with the following iDevice apps: *Twitter, FoodSpotting, Hipster, Instagram, Gowalla,* and *Foursquare*. Each identified app was placed, deployed and used on Plaintiff's iDevices before February 2012.

26. Plaintiff Nirali Mandaywala resides in Austin, Texas. Plaintiff Mandaywala owned and regularly used an iPhone with the following iDevice apps: *Instagram, Twitter, Yelp!, Gowalla,*

Foursquare, *Angry Birds Classic* and *Cut the Rope*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

27. Plaintiff Claire Moses resides in Austin, Texas. During the Class Period, Plaintiff Moses owned and regularly used an iPhone with the following iDevice apps: *Twitter* and *Instagram*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012.

28. Plaintiff Maria Pirozzi is a citizen of New Jersey and is an owner of an iPhone since September 2011. During that time, she has downloaded a number of apps from the App Store, including the *Facebook* and *Angry Birds* apps. Before purchasing her iPhone in September 2011, Pirozzi visited Apple's website as well as viewed Apple's in-store advertisements. In addition, Pirozzi relied on Apple's reputation for safety. Pirozzi purchased her iPhone with the expectation that she will be able to download and utilize apps available through the App Store without compromising the safety of her personal and private information. Indeed, Pirozzi purchased the iPhone for its apps feature with the expectation that she will download apps on her iPhone. Had Pirozzi known that Apple designed the iPhone in such a way as to make these devices vulnerable to unauthorized access from third-party apps, Pirozzi would not have downloaded apps and would have consequently paid less for her iPhone. At no time did Apple warn Pirozzi that her iPhone may be vulnerable to unauthorized access by third-parties.

29. Plaintiff Judy Paul resides in Austin, Texas. During the Class Period, Plaintiff Paul owned and regularly used an iPad and iPhone with the following iDevice apps: *Path, Foursquare, Gowalla, Twitter* and *Yelp!*. Each identified app was placed, deployed and used on Plaintiff's iDevices before February 2012.

30. Plaintiff Theda Sandiford resided in Austin, Texas. During the Class Period, Plaintiff Sandiford owned and regularly used an iPad and iPhone with the following iDevice apps: *Angry Birds Classic, Cut the Rope, FoodSpotting, Foursquare, Gowalla, Instagram* and *Yelp!*. Each identified app was placed, deployed and used on Plaintiff's iDevices before February 2012.

31. Plaintiff Greg Varner resides in Austin, Texas. During the Class Period, Plaintiff Varner owned and regularly used an iPhone with the following Apps: *Twitter, Instagram, Foursquare, Gowalla, Angry Birds Classic* and *Cut the Rope*. Each identified app was placed, deployed and used on Plaintiff's iDevice before February 2012. Plaintiff Varner has purchased multiple iPhones from 2007 onward. In particular, he purchased the original iPhone in or around 2007 or 2008, an iPad in or around 2008, the iPhone 3gs in 2009, the iPhone 4 in 2010, the iPhone 4s in 2011. He waited in line and purchased these iDevices at the Apple Store in Austin, Texas. Prior to making these purchases, he reviewed Apple's website and saw numerous in store, print and television ads concerning the products. He also watched all live blogs and web announcements in which the new iPhone products were discussed and launched. These blogs and web announcements include specifically those led by Steve Jobs and referenced herein. He continues to review these launches and announcements on line and intends to so again when the next launch is scheduled. Plaintiff Varner relied upon the information on Apple's website, ads, blogs and announcements in making his purchase. Based on the foregoing, Plaintiff Varner believed that the iPhone was a closed system, that Apple protected him from malware and malicious apps, and that his address book information was private and could not be taken without his consent. Had he known this to be false, Plaintiff Varner would not have purchased the above devices nor accepted apps from the App Store that uploaded or disclosed his mobile address book without his consent. Plaintiff Varner overpaid for the devices as a consequence of the above.

32. Before purchasing his or her iDevice, each Plaintiff visited Apple's website and viewed Apple's online, in-store, and/or television advertisements. In addition, each Plaintiff relied on Apple's reputation for safety, cultivated through Apple's extensive marketing and advertising campaigns. Each Plaintiff purchased an iDevice with the expectation that (i) it would come with a fully functioning App Store, and (ii) that Plaintiff would be able to utilize the "Contacts" function and iDevice apps from the App Store without compromising the security, safety, or control of Plaintiff's iDevice, mobile address book, or other personal and private information. Indeed, each Plaintiff purchased an iDevice with the expectation that he or she would maintain a mobile address

book and receive and use additional add-on apps on his or her iDevice. Had any Plaintiff known that iDevices lacked promised features or that Apple designed the iDevices with known vulnerabilities to unauthorized operations from Apple-issued [third-party] apps, Plaintiffs would not have accepted add-on apps from Apple or the App Store and would have paid less for his or her iDevice. At no time prior to the purchase of Plaintiffs' iDevice did Apple warn any Plaintiff that the iDevice and its data – particularly the Contacts feature and mobile address book – were vulnerable to unauthorized control and dissemination by third-parties.

Defendants

33. Defendant Apple is a California corporation licensed to do business in California and throughout the United States and has its principal place of business in Cupertino, California. Apple has appeared in this action. At all relevant times, Apple designed, manufactured, promoted, marketed, distributed, and/or sold the Apple iDevices throughout the United States and California. Apple also sells apps (including third party apps) for iDevices in the App Store and receives a portion of fees for apps that it sells in the App Store. The App Store is operated from Apple's offices in the United States. Apple also served as agent for each App Defendant with respect to the marketing, sale, deployment and account processing of their respective iDevice apps. Apple has already appeared in this action.

34. Defendant Chillingo Ltd. ("Chillingo") is a United Kingdom limited company with its principal place of business at Beechfield House, Winterton Way, Macclesfield, SK 11 OLP, United Kingdom. Chillingo was acquired by and became a division or wholly-owned, joint-reporting subsidiary of Defendant Electronic Arts Inc. around October 2010. Plaintiffs' claims against Chillingo arise, in whole or in part, out of business Chillingo conducted in California. Chillingo has done substantial business in California with Apple, Electronic Arts, and with Plaintiffs directly related to the *Angry Birds Classic* and *Cut the Rope* iDevice apps at issue in this case, which contain Chillingo's *Crystal* platform as an integral component. Apple, operating from California, marketed those apps to Plaintiffs and deployed those apps on the designated Plaintiffs' iDevices. Chillingo has already appeared in this action.

35. Defendant Electronic Arts Inc. ("Electronic Arts") is a Delaware corporation with its principal place of business in Redwood City, California and offices in Austin, Texas. Electronic Arts acquired Chillingo around October 2010, has operated Chillingo as a division or wholly-owned, joint-reporting subsidiary within Electronic Arts since then, and, on information and belief. is Chillingo's successor-in-interest. Electronic Arts has already appeared in this action.

36. Defendant Facebook, Inc. ("Facebook") is a Delaware corporation with its principal place of business in Menlo Park, California and offices in Austin, Texas. Facebook acquired Defendant *Instagram* for $1 billion in cash and stock in 2012 subsequent to the filing date of the above-captioned lead case. Facebook operated, supervised and controlled Defendant *Gowalla* Incorporated ("*Gowalla*") during portions of 2011 and 2012. On information and belief, Facebook is a successor-in-interest to *Gowalla*. Facebook has already appeared in this action.

37. Defendant Foodspotting, Inc. ("Foodspotting") is a Delaware corporation with its principal place of business at 526 2nd Street, San Francisco, California 94107. OpenTable, Inc., a NASDAQ-listed publicly-traded company, acquired Foodspotting in early 2013 for $10 million. Foodspotting has already appeared in this action.

38. Defendant Foursquare Labs, Inc. ("Foursquare Labs") is a Delaware corporation with its principal place of business at 36 Cooper Square, 6th Floor, New York, New York. Foursquare Labs has already appeared in this action.

39. Defendant *Gowalla* Incorporated ("*Gowalla*") is a Delaware corporation with its principal place of business at 610 W. 5th Street, Suite 604, Austin, Texas 78701. *Gowalla* was rendered insolvent or unable to satisfy creditor claims by its owners, management and Facebook via transactions in violation of California's Uniform Fraudulent Transfer Act. *Gowalla* has already appeared in this action.

40. Defendant Hipster, Inc. ("Hipster") is a Delaware corporation with its principal place of business at 330 Townsend Street, Ste. 202, San Francisco, California 94107. Subsequent to the filing of the Opperman action, Hipster, its personnel and/or its assets were acquired by America Online, Inc. ("AOL") on or around March 15, 2012. On information and belief, AOL is

successor-in-interest to Hipster. Hipster has already been served with process twice in the Opperman case through its registered Delaware agent for service of process, Agents and Corporations, Inc., 1201 Orange Street, Suite 600, One Commerce Center, Delaware 19801, but has not appeared and default has been entered against it on Opperman Plaintiffs' Second Amended Complaint. ECF Nos. 103, 346. Solely as against Hipster and in furtherance of that entry of default and to pursue default judgment, Plaintiffs from the *Opperman* case maintain and expressly incorporate herein the allegations and claims of their Second Amended Complaint, ECF No. 103, against Hipster. The present document is not intended to amend Plaintiffs' action against Hipster.

41. Defendant *Instagram*, Inc. is a privately held Delaware corporation headquartered at 181 South Park Avenue, San Francisco, California 94107.[4] *Instagram* does business throughout California and the United States. Defendant Facebook acquired *Instagram* for $1 billion subsequent to the filing of the Opperman action. *Instagram* has already appeared in this action.

42. Defendant Kik Interactive, Inc. ("Kik Interactive") is a Canadian corporation with its principal place of business at 420 Weber St. North, Unit I, Waterloo, N2L 4E7, Canada. Plaintiffs' claims against Kik Interactive arise, in whole or in part, out of the business Kik Interactive conducted in California. Kik Interactive has done substantial business in California with Apple since 2010 and with Plaintiffs directly related to the Kik Messenger iDevice app at issue in this case. For instance, Kik Interactive appointed Apple as its agent on the *Kik Messenger* iDevice App. Apple, operating from California and in furtherance of its role as Kik Interactive's agent, marketed the *Kik Messenger* iDevice app to Plaintiffs and deployed the *Kik Messenger* app on the designated Plaintiffs' iDevices. Kik Interactive has already appeared in this action.

[4] For purposes of this Complaint, *Instagram*, Inc. includes the related and/or predecessor corporate entities of *Instagram*, LLC, Burbn, Inc., and Instagr.am. *Instagram* is successor-in-interest to Burbn, Inc., a Delaware corporation which had its principal place of business at 265 Rivoli Street 4, San Francisco, California 94105.

43. Defendant Path, Inc. ("Path") is a privately held Delaware corporation headquartered at 301 Howard Street, Suite 2200, San Francisco, California 94105. Path does business throughout California and the United States. Path has already appeared in this action.

44. Defendant Rovio Entertainment, Ltd. s/h/a Rovio Mobile Oy ("Rovio") is a Finland corporation with its principal place of business at Keilaranta 19 D 02150, Espoo, Finland. Plaintiffs' claims against Rovio arise, in whole or in part, out of the business Rovio conducted in California. Rovio has done substantial business in California with Apple and with Plaintiffs directly related to the *Angry Birds Classic* iDevice app at issue in this case. For instance, Rovio appointed Apple, either directly or indirectly, as its agent on the *Angry Birds Classic* iDevice App. Apple, operating from California and in furtherance of its role as Rovio's agent, marketed the *Angry Birds Classic* iDevice app to Plaintiffs and deployed the *Angry Birds Classic* app on the designated Plaintiffs' iDevices. Rovio has already appeared in this action.

45. Defendant Twitter, Inc. ("Twitter") is a Delaware corporation with its principal place of business at 795 Folsom Street, Suite 600, San Francisco, California 94107. Twitter has already appeared in this action.

46. Defendant Yelp! Inc. ("Yelp") is a Delaware corporation with its principal place of business at 706 Mission Street, San Francisco, California 94103. Yelp has already appeared in this action.

47. Defendant ZeptoLab UK Limited aka ZeptoLab ("ZeptoLab") is a United Kingdom limited company with its principal place of business at 11 Staple Inn Buildings, London, United Kingdom WC1V7QH. Plaintiffs' claims against ZeptoLab arise, in whole or in part, out of the business ZeptoLab conducted in California. ZeptoLab has done substantial business in California with Apple, with Chillingno and Electronic Arts, and with Plaintiffs directly related to the *Cut the Rope* iDevice app at issue in this case. ZeptoLab appointed Apple as its agent, either directly or indirectly, on the *Cut the Rope* iDevice App. Apple, operating from California and in furtherance of its role as ZeptoLabs' agent, marketed the *Cut the Rope* iDevice app to Plaintiffs and deployed

the *Cut the Rope* app on the designated Plaintiffs' iDevices. ZeptoLab has already appeared in this action.

CLASS ACTION ALLEGATIONS

48. Plaintiffs bring this lawsuit as a class action under Rules 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3) of the Federal Rules of Civil Procedure on behalf of a Class of similarly situated persons consisting of:

> **The iDevice Class**: Plaintiffs and all persons who purchased iDevices between July 10, 2008 and the present and downloaded apps to these devices.
>
> **The Malware Subclass**: Each Plaintiff and all members of the iDevice Class who received the *Angry Birds Classic* (with integrated *Crystal* platform), *Cut the Rope* (with integrated *Crystal* platform), *Foursquare, Foodspotting, Gowalla, Hipster, Kik Messenger, Instagram, Path, Twitter,* or *Yelp!* iDevice Apps from Apple before February 5, 2012.
>
> **The Address Book Subclass**: Each Plaintiff and all members of the Malware Class whose iDevice, without requesting prior approval to do so and as a result of the *Angry Birds Classic* (with integrated *Crystal* platform), *Cut the Rope* (with integrated *Crystal* platform), *Foursquare, Foodspotting, Gowalla, Hipster, Kik Messenger, Instagram, Path, Twitter,* or *Yelp!* iDevice apps, transmitted, disclosed and/or disseminated the iDevice's mobile address book (or substantial portions thereof) over the Internet and/or to third-parties.[5]
>
> [**The Texas Subclass**: Each Plaintiff and all members of the Address Book Subclass who resided in Texas when the mobile address book transmission occurred.

Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint. Defendants, their subsidiaries, their officers, directors, managing agents and members of those persons' immediate families, the Court, Court personnel, and legal representatives, heirs, successors or assigns of any excluded person or entity are excluded from the Class.

49. **Numerosity.** The members of the Class, who are ascertainable from Defendants' records, are so numerous that joinder of all members is impracticable. The Class is likely to exceed five million members from reported iDevice sales figures and reported user bases for the identified

[5] Discovery in the case may indicate the appropriateness of app-specific subclasses for both the Malware and Address Book subclasses.

apps. Disposition of this matter as a class action, instead of separate actions, will be substantially more efficient, economical and practical for the parties and the Court and will avoid inconsistent or conflicting decisions.

50. **Typicality.** Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs and all members of the Class purchased an Apple iDevice, maintained his or her private mobile address book and photographs with that iDevice, received one or more identified iDevice apps from Apple, and have sustained damages arising out of Defendants' conduct.

51. **Commonality.** Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members. Issues of law and fact common to the Class include:

- Defendants' marketing and statements about iDevices and apps;
- The marketing, development and sales channels for iDevice apps;
- Applicable standards of care;
- Communications between or directed towards the parties;
- iDevice purchasers' privacy and ownership interests in their iDevices and mobile address books;
- The presence of computer contaminants, malware or spyware in the identified apps;
- The absence of security features in and the defective design of Apple iDevices;
- The App Defendants' acquisition, use, retention and public disclosure of iDevice owners' mobile address books;
- The business conducted through and policies and procedures pertaining to the iOS App Developer Program and/or the App Store;
- Knowledge, intent, malice or recklessness associated with Defendants' acts and conduct;
- The interpretation and effect of any disclosures, guidelines, policies, agreements, or on-device alerts or pop-up dialogue boxes;
- Which state and federal laws Defendants violated including whether Apple (i) violated the UCL, Cal. Bus. Prof. Code §17200, *et seq.*; (ii) violated the FAL, Cal. Bus. Prof. Code §17500, *et seq.*; (iii) violated the CLRA, Cal. Civ. Code. §1750 *et seq.*; and (iv) made negligent misrepresentations to the Class; and whether Apple misled purchasers about the true nature of the iDevices, the App Store, and third-party apps;

- Valuation methods for mobile address books and the "contacts data" points and fields contained therein;
- The proper measure and amount of damages, including statutory awards; and
- The unjust benefits realized by any Defendants.

52. **Adequacy.** Plaintiffs will continue to fairly and adequately represent the interests of the Class and have no interests adverse to or in conflict with other Class Members. Plaintiffs' retained counsel have and will continue to vigorously prosecute this case, have previously been designated class counsel on cases in this judicial district, and are highly experienced in class and complex, multi-party litigation matters, including those centered on computer, networking, Internet and communications technologies, tangible and intangible property rights, privacy and Constitutional rights, electronic piracy and RICO violations, and consumer matters. Already as a result of Plaintiffs' and their counsels' prosecution of this case to date, Path began anonymizing and encrypting transmitted user mobile address book materials and Apple imposed new technical barriers to impede the access or transmission of iDevice mobile address books in the absence of prior notification to and approval from the iDevice owner.

53. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy since, among other things, joinder of all Class Members is impracticable and a class action will reduce the risk of inconsistent adjudications or repeated litigation on the same conduct. Further, the expense and burden of individual lawsuits would make it virtually impossible for Class Members, Defendants, or the Court to cost-effectively redress separately the unlawful conduct alleged. Thus, absent a class action, Defendants would unjustly retain the benefits of their wrongdoings. Plaintiffs know of no difficulties to be encountered in the management of this action that would preclude its maintenance as a class action, either with or without sub-classes.

54. The claims asserted herein are applicable to all individuals and entities throughout the United States who purchased an iDevice and/or obtained the identified apps. The State of California has sufficient state interest through a significant contact or aggregation of contacts to the

claims asserted by each member of the Class so that the choice of California law is not arbitrary or unfair.

55. Adequate notice can be given to Class members directly using information maintained in Apple's and other Defendants' records, or through notice by publication.

56. Accordingly, class certification is appropriate under Rule 23.

SUBSTANTIVE ALLEGATIONS[6]

57. Apple launched the App Store in 2008 concurrently with the launch of its third-generation iPhone, the iPhone 3G. Apple heavily promoted the App Store with its "There's an App for That" ad campaign. The campaign encouraged iPhone purchasers to download apps from the App Store. For example, Apple's "Dilemmas" commercial encouraged users to download the app UrbanSpoon – which allows users to search for nearby restaurants – with a tagline "the iPhone. Solving life's dilemmas one app at a time." In promoting apps in July 2008, Apple's website provided:

> ***Applications unlike anything you've seen on a phone before.***
>
> Applications designed for iPhone are nothing short of amazing. That's because they leverage the groundbreaking technology in iPhone — like the Multi-Touch interface, the accelerometer, GPS, real-time 3D graphics, and 3D positional audio. Just tap into the App Store and choose from over 500 applications ready to download now.

58. Apple's strong promotion of the App Store proved successful. In the first week of the App Store's launch, Apple reported that users already downloaded more than 10 million apps from the App Store:

> "The App Store is a grand slam, with a staggering 10 million applications downloaded in just three days," said Steve Jobs, Apple's CEO. "Developers have created some extraordinary applications, and the App Store can wirelessly deliver them to every iPhone and iPod touch user instantly."

[6] The allegations in this section were previously sustained by the Court in connection with the Pirozzi Complaint in support of claims for violation of the UCL, the FLA, the CLRA and Negligent Misrepresentation.

See July 14, 2008 press release (available at www.apple.com). Today, Apple boasts that the App Store has over 700,000 apps for iPhone and iPod touch and 275,000 apps for the iPad. On January 7, 2013, Apple announced that, since 2008, customers have downloaded over 40 billion apps – nearly 20 billion in 2012 alone. *See* January 7, 2012 press release (available at www.apple.com). Apple heavily encourages purchasers to download apps. For example, since the inception of the App Store, Apple has told consumers "[t]he more apps you download, the more you realize there's almost no limit to what your iPhone can do" and has made similar representations regarding the iPad and the iPod touch.

59. Not surprisingly, the availability of apps has been credited with propelling the popularity of the iDevices. Apps are not only an integral part of the iDevices themselves, but are the key feature that has differentiated iDevices from similar products.

60. The App Store is under Apple's exclusive domain and the company has ultimate control of what apps are available for purchase or download by consumers. Furthermore, Apple has designed the iDevices to accept apps only from the App Store.

61. Each iDevice comes pre-programmed with certain built-in apps created by Apple. These Apple apps cannot be deleted from the iDevice. The App Store is one of such built-in apps and provides iDevice purchasers with instant access to any app available through the App Store. Similarly, additional built in apps include the Photos app (where users can store personal photographs and videos) as well as the Contacts app.[7]

62. Plaintiffs and other members of the proposed Class downloaded apps to their iDevice from the App Store as part of the use of their mobile devices. Apple claims to review each application before offering it to its users, purports to have implemented apps privacy standards, and claims to have created a strong privacy protection for its customers. However,

[7] In addition to storing Photos, the Photos app also stores information about when and where the photo was taken. The Contacts app allows users to customize contacts information using the following fields: (1) first and last name and phonetic spelling of each, (2) nickname, (3) company, job title and department, (4) address(es), (5) phone number(s), (6) e-mail address(es), (7) instant messenger contact, (8) photo, (9) birthday, (10) related people, (11) homepage, (12) notes, (13) ringtone, and (14) text tone.

unbeknownst to consumers such as Plaintiffs some of these apps have been accessing and/or uploading information from other apps located on the iDevices, including, but not limited to, user name and contact information, detailed contacts list stored in the Contacts app, photographs, and videos without user knowledge or consent. For example, users who allow apps to use location data are also unknowingly giving these apps access to the user's private photo and video files that can be uploaded and saved on the app's servers. Similarly, users who use an app's "find friends" feature unwittingly allowed these apps to access and download users' entire address book and contacts list.

63. Apple failed to properly safeguard iDevices and, instead, induced Plaintiffs and members of the Class to purchase iDevices and to download apps under the premise that users' private information would remain confidential and would not be shared with third-party developers without express consent.

64. Apple has repeatedly represented that Apple's products are safe and secure, and that private information could not be accessed by third-party apps without the user's express consent. Plaintiffs purchased their iDevices with the expectation that Apple designed the iDevices to protect user privacy and would not have purchased their iDevices and/or would have paid less for the iDevices had they known the truth about the iDevices. Instead, Plaintiffs have learned that third-party apps are capable of accessing private user data such as users' photos, videos, and contacts without user consent. Plaintiffs allege that Apple designed the iDevices in such a way as to make these devices vulnerable to unauthorized access by third-parties, despite their misrepresentations that such access was impossible. Apple's failure to disclose that third-party apps had the ability to access private photo and contact information resulted in harm to Plaintiffs and the Class. Plaintiffs purchased their iDevices with the expectation that their private information would remain safe and would not have paid as much for their iDevices if they knew that Apple did not properly safeguard these devices.

The Apple Devices

65. Apple designs both the hardware component of the Apple Devices as well as the operating system (the iOS) that runs each device.

66. The iPhone is the most popular of the three devices. For example, in 2011 and 2012, Apple sold 72 million and 125 million iPhones respectively. Apple sold approximately 11 million and 8 million iPod touches and 32 million and 58 million iPads in the same time period.

67. The iPod touch is a portable digital music and media player based on Apple's proprietary iOS and includes a multi-touch interface and the App Store.

68. The iPhone combines a mobile phone, an iPod touch, and an internet communication device into a single hand-held product. The iPhone is therefore more than simply a phone and Apple's marketing of the iPhone has focused not on its ability to make phone calls, but on the availability and utility of third-party apps. Indeed, since the launch of the App Store, Apple's Annual Reports to shareholders have cautioned that "[t]he Company believes decisions by customers to purchase its hardware products depend in part on the availability of third-party software applications and services for the Company's products…with respect to iOS devices, the Company relies on the continued availability and development of compelling and innovative software applications, which are distributed through a single distribution channel, the App Store."

69. The iPad is a multi-purpose mobile device. Like the iPhone and the iPod touch, the iPad is based on the company's multi-touch technology and comes installed with the App Store. The iPhone, iPod touch and the iPad share many of the same apps.

70. The price of each iDevice depends on the available memory on the device measured in gigabytes (GB). Apple sells a locked iPhone starting at $199 for a 16GB phone, $299 for a 32GB phone, and $399 for a 64GB phone.[8] Thus, Apple sells additional memory at a

[8] A locked phone is one that comes with a two-year wireless plan from a wireless provider such as AT&T, Verizon and Sprint. These wireless providers subsidize some of the cost of the phone through the two-year plan. An "unlocked" phone without a wireless contract is more costly. For example, an unlocked 16GB phone costs $649, a 32GB phone costs $749, and a 64GB phone costs $849.

premium, telling consumers, "[t]he more gigabytes you have, the more content you can store on your iPhone – apps, photos, HD videos, music, movies and more."

71. Similarly, Apple charges a premium for additional space on the iPad: $499 for the 16GB iPad, $599 for the 32GB iPad, and $699 for the 64GB iPad. As with the iPhone, Apple encourages consumers to purchase an iPad with a larger capacity.

72. Finally, the iPod touch is priced at $199 for 16GB, $299 for 32GB and $399 for 64GB.

73. Thus, it appears that, after the first 16GB of memory, every additional 16GB of memory space is worth approximately $100. Every app takes up a portion of the available memory on the iDevice depending on the size of the app.

The App Store

74. In July 2008, Apple launched the App Store where customers can shop for and download apps offered by Apple and third-party developers. The launch of the App Store coincided with the launch of Apple's iPhone 3G. In the first week of the App Store's launch, Apple reported that users already downloaded more than 10 million apps from the App Store.

75. When it first launched, the App Store contained only about 500 apps. At the initial drafting of this Complaint, the App Store had over 500,000 third-party applications covering a wide variety of areas including games, news, health, travel, education, business, sports, and social networking:

> Over 500,000 apps. For work, play, and everything in between. The apps that come with your iPhone are just the beginning. Browse the App Store to find hundreds of thousands more. The more apps you download, the more you realize there's almost no limit to what your iPhone can do.

76. Apple makes similar claims regarding iPad and iPod Touch. With regards to the iPad, Apple provided at the time of the initial filing of Plaintiff's Complaint:

> An app made for iPad is an app like no other. That's because apps for iPad are designed specifically to take advantage of all the technology built into iPad. And with over 200,000 apps to choose from, there's no telling where the next tap will take you.

77. Today Apple boasts 700,000 apps in the App Store for the iPhone/iPod touch and 275,000 apps designed specifically for the iPad.

78. Apple has designed its iPhone, iPad and iPod Touch wireless mobile devices to accept apps only from the App Store, making the App Store the exclusive source from which consumers may obtain apps for their iDevices.

79. Since July 2008, over 40 billion apps have been downloaded by customers using iDevices. In 2011 alone, Apple sold 72.3 million iPhone handsets, 32.4 million iPads and approximately 11 million iPod touches. By 2012, Apple's iPhone sales increased to 125 million units, iPad sales rose to 58 million units and iPod touch sales fell to approximately 8 million units.[9]

80. The App Store had $1.782 billion in revenues in 2010 and $6.9 billion in revenues in 2011 and was on track to generate over $9 billion for calendar year 2012. News reports estimate that by 2016, total mobile app revenues will reach a staggering $22.4 billion. While Apple shares app revenue with developers, Apple nevertheless profits from the apps directly through sales and, more importantly, through the increased popularity of its mobile devices. For example, Apple reported third-party app sales were one of the primary contributors to the $13.8 billion increase in Apple's net sales for its America segment in 2011 along with the higher sales of the iPhone.

81. In addition to making the availability of apps for the iDevices one of the key components of its advertising and marketing strategy for the iDevices to drive the sales of the iDevices, Apple has encouraged purchasers to pay for additional memory when purchasing such devices in part because "[t]he more gigabytes you have, the more content you can store on your iPhone – apps, games, photos, HD videos, music, movies, and more."

[9] Apple does not traditionally report unit sales specifically for the iPod touch in its filings with the U.S. Securities and Exchange Commission. However, Apple released iPod touch sales in connection with a lawsuit with Samsung.

82. Indeed, many have described the App Store as a game changer both for Apple and for smart phones in general. According to one Morgan Stanley analyst, "Apple changed the view of what you can do with that small phone in your back pocket….Applications make the smartphone trend a revolutionary trend — one we haven't seen in consumer technology for many years."

83. Apps are an integral part of the iDevices and have propelled Apple and iDevices' popularity. According to a NEW YORK TIMES article entitled, "Apple's Game Changer, Downloading Now":

> One need not look further than the lobby of Apple's headquarters in Cupertino, Calif., to see that the iPhone and applications that run on it are centerpieces of the company's mobile strategy. Planted squarely in the lobby of the main office, at 1 Infinite Loop, is an impressive, 24-foot-wide array built out of 20 LED screens populated with 20,000 tiny, brightly colored icons.
>
> As Philip W. Schiller, head of worldwide product marketing at Apple, describes how the wall works — each time an application is purchased, the corresponding icon on the electronic billboard jiggles, causing its neighbors to ripple in unison — he, too, becomes animated.
>
> Normally reserved and on message, Mr. Schiller waves his hands back and forth and allows his voice to ascend into giddy registers as he speaks about the potential unleashed by the App Store.
>
> "I absolutely think this is the future of great software development and distribution," Mr. Schiller says. "The idea that anyone, all the way from an individual to a large company, can create software that is innovative and be carried around in a customer's pocket is just exploding. It's a breakthrough, and that is the future, and every software developer sees it." (available at http://www.nytimes.com/2009/12/06/technology/06apps.html?pagewanted=all).

84. Apple's reliance on apps to drive the sale of Apple Devices has been readily recognized by the company itself, which provides in its 2012 Annual Report:

> ***The Company's future performance depends in part on support from third-party software developers.***
>
> The Company believes decisions by customers to purchase its hardware products depend in part on the availability of third-party software applications and services. There is no assurance that third-party developers will continue to develop and maintain software applications and services for the Company's products. If third-party software applications and services cease to be developed and maintained for the Company's products, customers may choose not to buy the Company's products.
>
> * * *

> With respect to iOS devices, the Company relies on the continued availability and development of compelling and innovative software applications, which are distributed through a single distribution channel, the App Store.

85. Similarly, in its 2011 Annual Report, Apple disclosed that:

> ***The Company's future performance depends in part on support from third-party software developers.***
>
> The Company believes decisions by customers to purchase its hardware products depend in part on the availability of third-party software applications and services. There is no assurance that third-party developers will continue to develop and maintain software applications and services for the Company's products. If third-party software applications and services cease to be developed and maintained for the Company's products, customers may choose not to buy the Company's products, which could materially adversely affect the Company's financial condition and operating results.

86. Thus, Apple has a keen interest in continuing to promote iDevices without disclosing that apps are capable of and are collecting private data without user consent. As Apple has recognized in its Annual Report, the company faces significant competition in the mobile communication and media device industry and attracting third-party app manufacturers and consumers are a key to the company's future:

> The Company markets certain mobile communication and media devices based on the iOS mobile operating system and also markets related third-party digital content and applications. The Company faces substantial competition in these markets from companies that have significant technical, marketing, distribution and other resources, as well as established hardware, software and digital content supplier relationships. Additionally, the Company faces significant price competition as competitors reduce their selling prices and attempt to imitate the Company's product features and applications within their own products or, alternatively, collaborate with each other to offer solutions that are more competitive than those they currently offer.

The Application Process

87. Apple is notorious for complete control over its products. Apple's former Chief Executive Officer ("CEO"), Steve Jobs has publicly stated, "our job is to take responsibility for the complete user experience. And if it's not up to par, it's our fault, plain and simply."

88. To that end, Apple has designed iDevices to accept apps only from the App Store, thereby making the App Store the exclusive source from which consumers may obtain apps for their iDevices whether or not the apps are sold or available for free. The only exception to this restriction are devices that are modified by users to circumvent the iOS operating system's

restrictions on downloading apps from sources other than the App Store, a process known as iOS jailbreaking or jailbreaking. While jailbreaking iDevices is legal, Apple has sought to discourage jailbreaking by announcing that the practice voids the iDevices' warranty.

89. In order to offer an application for download in the App Store, a third-party developer must be registered as an "Apple Developer" and agree to the iOS Developer Agreement (the "IDA") and the Program License Agreement (the "PLA") with Apple as well as pay a $99 yearly registration fee. Apple provides third-party developers with review guidelines, and conducts a review of all applications submitted for inclusion in the App Store for compliance with these documents.

90. To get applications into the App Store, Apple requires developers to submit their app and wait for approval or rejection by Apple (and rejected apps are given feedback on the reason they were rejected so they can be modified and resubmitted). Apple has the sole discretion over the app approval process and may reject a proposed app for any reason. Apple may further unilaterally choose to cease distributing any app at any time and for any reason. Apple has explicitly reserved the right to cease distributing any app that, among other things, (i) breaches the terms and conditions of the licensing agreements, (ii) provides Apple with inaccurate documents or information, or (iii) Apple has been notified or has reasons to believe that the app violates, misappropriates, or infringes the rights of a third party.

91. In addition to having exclusive control of the apps offered for sale or download at the App Store, Apple controls the app development process. For example, App developers must buy and use Apple's software development kit, which provides highly detailed guidelines for app development.

92. Apple therefore acts as a gatekeeper to the App Store. Indeed, when Apple first launched the App Store, Steve Jobs stated, "[t]here are going to be some apps that we're not going to distribute. Porn, malicious apps, apps that invade your privacy." (http://cnettv.cnet.com/jobs-unveils-iphone-app-store/9742-1_53-32454.html).

93. Jobs further made this clear at an iPhone SDK (or Software Developer Kit) Press Conference on March 6, 2008 showing the limitations on the type of apps that would be allowed on the iPhone:

94. In October 2007 Jobs similarly stated:

> Let me just say it: We want native third party applications on the iPhone, and we plan to have an SDK in developers' hands in February. We are excited about creating a vibrant third party developer community around the iPhone and enabling hundreds of new applications for our users. It will take until February to release an SDK because we're trying to do two diametrically opposed things at once — provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. As our phones become more powerful, these malicious programs will become more dangerous, and since the iPhone is the most advanced phone ever, it will be a highly visible target. We think a few months of patience now will be rewarded by many years of great third party applications running on safe and reliable iPhones.

95. Apple has echoed this sentiment on several occasions. For example, in 2010, the Company's cracked down on apps that contained "overtly sexual" content and removed several such apps from the App Store according to THE NEW YORK TIMES:

> Philip W. Schiller, head of worldwide product marketing at Apple, said in an interview that over the last few weeks a small number of developers had been submitting "an increasing number of apps containing very objectionable content."
>
> "It came to the point where we were getting customer complaints from women who found the content getting too degrading and objectionable, as well as parents who were upset with what their kids were able to see," Mr. Schiller said.

96. Likewise, Jobs, who often responded to user emails, wrote in a much publicized email responding to a reporter's question: "Yep, freedom from programs that steal your private

data. Freedom from programs that trash your battery. Freedom from porn. Yep, freedom. The times they are a changin', and some traditional PC folks feel like their world is slipping away. It is." Jobs further said, "We believe we have a moral responsibility to keep porn off the iPhone. Folks who want porn can buy an Android."

97. Apple has also famously refused to integrate Adobe Flash technology (which is utilized by many websites and without which iDevices cannot access such content) despite users' requests, with Jobs explaining (on Apple's website in April 2010) that Apple will not integrate Adobe's flash technology because of reliability, security, and performance concerns.

98. Likewise, on April 20, 2011, the company's current CEO, Timothy Cook, noted that users appreciate Apple's gatekeeper function, stating "I think the user appreciates that Apple can take full responsibility for their experience…" (http://articles.businessinsider.com/2011-04-20/tech/29957463_1_google-android-ios-iphone).

99. In sum, Apple has attempted to cultivate a perception that its products are safe and that Apple strives to protect users.

100. Apple completely controls users' experience from development of the iDevice, development and selection of the apps available at the App Store, as well as restriction of how the iDevice can be modified by users (e.g., such as blocking users from modifying their devices or installing unapproved software on their Apple Devices). Apple further restricts information concerning the development process and prohibits developers from publicly discussing Apple's standards for app development through the PLA.

101. The App Store Review Guidelines set forth the technical, design, and content guidelines Apple will use when reviewing an app for inclusion in Apple's App Store. These guidelines state that apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." This includes the transmission of personally identifiable information. In addition, the requirements of the PLA empower users to control access to user or device data, and require user consent before user or device data can be collected.

102. According to Apple, its operating system, iOS, "is highly secure from the moment you turn on your iPhone." For example, in September 2011, Apple's website provided:[10]

Safe and secure by design.

iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information. Optional parental controls let you manage iTunes purchases, Internet browsing, and access to explicit material. To guard your privacy, apps requesting location information must get your permission first. You can set a passcode lock to prevent unauthorized access to your phone and configure iPhone to delete all your data after too many unsuccessful passcode attempts. And in the event your iPhone is lost or stolen, Find My iPhone allows you to locate it on a map, lock its screen, and remotely delete all your data. If you get it back, you can restore everything from your last backup.

103. Apple makes similar claims with respect to the iPad and the iPod Touch.

104. Indeed, according to the App Store's development guidelines, "[t]he app approval process is in place to ensure that applications are reliable, perform as expected, and are free of explicit and offensive material. We review every app on the App Store based on a set of technical, content, and design criteria." Since 2010, App Store's guidelines provided that "Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." The guidelines

---

[10] (the text reads): Safe and secure by design.

iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information. Optional parental controls let you manage iTunes purchases, Internet browsing, and access to explicit material. To guard your privacy, apps requesting location information must get your permission first. You can set a passcode lock to prevent unauthorized access to your phone and configure iPhone to delete all your data after too many unsuccessful passcode attempts. And in the event your iPhone is lost or stolen, Find My iPhone allows you to locate it on a map, lock its screen, and remotely delete all your data. If you get it back, you can restore everything from your last backup.

further provided that "Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected."

105. With respect to location-based services, the Apple privacy policy provides only that the company may obtain anonymous location data that does not personally identify the user:

> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.

106. In February 2012, an Apple spokesperson, Tom Neumayr, further reaffirmed that "apps that collect or transmit a user's contact data without their prior permission are in violation of our guidelines."

Despite Apple's Promises to Safeguard Users' Privacy, Apps Have Been Surreptitiously Collecting User Data

107. In contrast to Apple's statements, Apple-approved apps have accessed, downloaded and/or copied users' private contacts information, location data, private photographs and videos without the users' knowledge or consent when a user agrees to allow an app to access the user's then current locations.

108. For example, when an app such as Defendant Rovio's Angry Birds[11] asks purchasers to use their current location, in addition to using the purchaser's location, the app is able to gain access to other apps such as the Photos app. This is in direct contravention to Apple's representation that its iOS is safe and secure and that "All apps run in a safe environment, so a website or app can't access data from other apps." Similarly, two app manufacturers acknowledged that they had surreptitiously accessed and uploaded information from users' Contacts app through a "Find Friends" feature without disclosing to users that the feature would

[11] A popular game that take advantage of iDevices' touch interface and involves launching of cartoon birds at various obstacles.

leave their private information vulnerable to unauthorized download by the third-party app manufacturer.

109. These uses go well beyond what a reasonable iDevice user understands himself or herself to be consenting to when he or she allows an app to access data on the iDevice for the app's functionality.

110. For example, in early February 2012, it was uncovered that one such app, Path, was uploading data stored on users' iDevices (including address book and calendar) to its servers, causing the app developers' CEO to issue an apology to Path users:

> **We are sorry**
>
> We made a mistake. Over the last couple of days users brought to light an issue concerning how we handle your personal information on Path, specifically the transmission and storage of your phone contacts.
>
> As our mission is to build the world's first personal network, a trusted place for you to journal and share life with close friends and family, we take the storage and transmission of your personal information very, very seriously.
>
> Through the feedback we've received from all of you, we now understand that the way we had designed our 'Add Friends' feature was wrong. We are deeply sorry if you were uncomfortable with how our application used your phone contacts.
>
> In the interest of complete transparency we want to clarify that the use of this information is limited to improving the quality of friend suggestions when you use the 'Add Friends' feature and to notify you when one of your contacts joins Path--nothing else. We always transmit this and any other information you share on Path to our servers over an encrypted connection. It is also stored securely on our servers using industry standard firewall technology.
>
> We believe you should have control when it comes to sharing your personal information. We also believe that actions speak louder than words. So, as a clear signal of our commitment to your privacy, we've deleted the entire collection of user uploaded contact information from our servers. Your trust matters to us and we want you to feel completely in control of your information on Path.
>
> In Path 2.0.6, released to the App Store today, you are prompted to opt in or out of sharing your phone's contacts with our servers in order to find your friends and family on Path. If you accept and later decide you would like to revoke this access, please send an email to service@path.com and we will promptly see to it that your contact information is removed.
>
> We care deeply about your privacy and about creating a trusted place for you to share life with your close friends and family. As we continue to expand and grow we will make some mistakes along the way. We commit to you that we will continue to be transparent and always serve you, our users, first.

> We hope this update clears up any confusion. You can find Path 2.0.6 in the App Store here.
>
> Sincerely,
> Dave Morin
> Co-Founder and CEO

(available at: http://news.cnet.com/8301-19882_3-57373474-250/path-ceo-we-are-sorry-and-weve-deleted-your-address-book-data/).

111. Likewise, other popular apps such as Angry Birds, Cut-the-Rope, Twitter, Facebook, LinkedIn, *Gowalla*, *Foodspotting*, *Instagram*, *Foursquare*, *Beluga*, *Yelp!*, *Hipster and Kik Messenger* among others, have likewise downloaded users' data without their explicit consent in contrast to Apple's stated policy.

112. Following revelations that Path secretly uploaded user data, one user, Mark Chang, found that another app, Hipster, also uploads users' address books to its servers:

> **Hipster uploads part of your iPhone address book to its servers**
>
> Inspired by this post (which you should all read), I looked at the apps on my own iPhone for information leakage by other apps. I figured this would be common practice, and lo and behold, when booting up Hipster, it seems like parts of my iPhone address book were being uploaded to Hipster. Here's the breakdown, done in the style of Arun Thampi (the author of the first post).
>
> Creating an Account
>
> Hipster starts with a POST to api.hipster.com/v1/people
>
> Worth noting, this is not over HTTPS, and it sends your info, including password and iPhone UID in plaintext. Ugh.

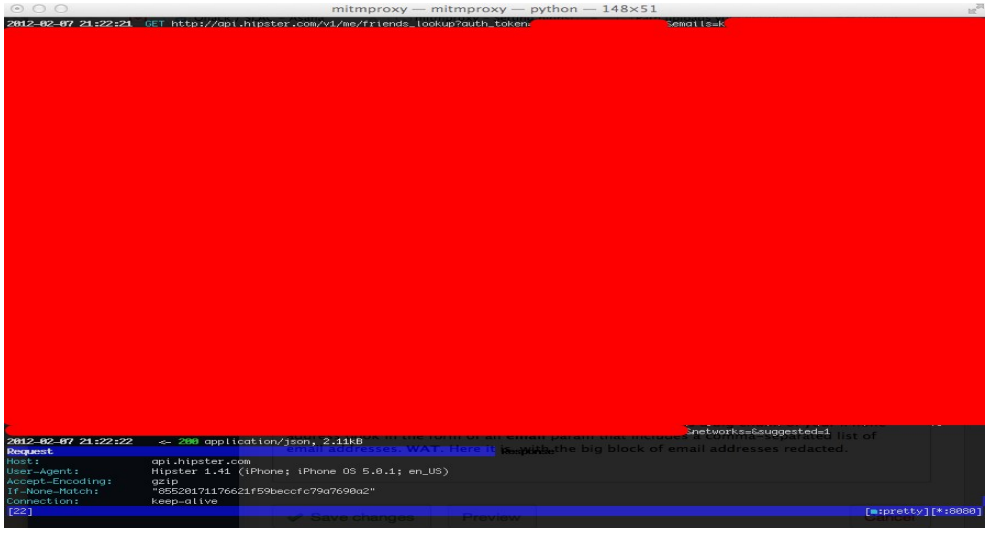
Okay, not terrible.

Several other transactions happen here, giving us acknowledgment of your login and creation of an account and user ID, and the public "Popular" feed is returned.

Sadly, the badness happens when you go to add your friends from the More > Find Friends menu option.

Badness

The Hipster app, in an unsecured HTTP GET request, sends a big chunk of your iPhone address book in the form of an email param that includes a comma-separated list of email addresses. WAT. Here it is, with the big block of email addresses redacted.



Okay, that's enormous. Let's just get the important bits. The HTTP GET goes to: api.hipster.com/v1/me/friends_lookup?auth_token=[redacted]&emails=[…]

Boy. Thanks, Hipster.

The Issue

As was addressed in the other post, this is offensive for a few reasons:

1. Hipster never asked me for permission to send my address book emails to them.
2. Hipster does not say anything (AFAIK) about if they are storing those emails or what.
3. The Hipster app allows you to deselect the "Contacts" button when looking for new friends, but it is enabled by default. Therefore, there is no way to avoid sending address book emails to Hipster, as far as I can tell.

* * *

(available at: http://markchang.tumblr.com/post/17244167951/hipster-uploads-part-of-your-iphone-address-book-to-its).

113. In response to Chang's article, on February 8, 2012, Hipster's CEO, Doug Ludlow, quickly posted an apology to Hipster's users:

> We blew it, we're sorry, and we're going to make it right.
>
> It's Hipster's goal to provide a fun and beautiful service for our community to share where they are, and what they are doing – creating a safe environment for our users is of the utmost importance to us. However, when we built our "Find Friends" feature for iOS, we clearly dropped the ball when it comes to protecting our users' privacy.
>
> Yesterday, one of our Hipster users, Mark Chang (http://markchang.tumblr.com/) wrote a blog post detailing a few ways in which our "Find Friends" feature handles user privacy issues. You can read his post here.
>
> Mark's criticisms were spot on, and needless to say we're pretty embarrassed by the situation. Embarrassed not because we had malicious goals in mind (we don't store the contact data we pull – we just match it to existing users), but embarrassed by the fact that we pushed a feature that doesn't meet our standards for the protection of our user's data.
>
> How are we working to remedy the situation? In an update that will be available through iTunes this week, we've changed the way our "Find Friends" feature works on iOS. Rather than automatically pull in a user's contacts to help them find people already on Hipster, we're making this feature opt-in, and users will have to confirm that they want to grant access to their address book. In addition, this data will now be transferred through a SSL connection.
>
> But where do we go from here?
>
> We'd like to use our recent experience to help improve the mobile industry as a whole.
>
> On Thursday, February 17th, we'll be hosting a "Application Privacy Summit" here at Hipster's SF office to discuss of user privacy in mobile applications. In addition to discussing best practices and privacy standards, the goal of the summit to be to come up with a "privacy pledge" – one that can be adopted by all apps, detailing for users what types of privacy expectations they should have. Applications will be able to boast that they have agreed to the privacy pledge, which should help give their users sense of mind regarding their personal data.
> Invitations are being sent out to the CEOs of major mobile application companies, and we hope they will attend. In addition, if you're interested in attending, please email me at Doug@Hipster.com.
>
> We made a mistake, but we hope that what we've learned will shed light on the need for clear standards when it comes to protecting user privacy. Doing so will only do great things for our industry, our companies, and most importantly, our users.

(available at: http://techcrunch.com/2012/02/08/hipster-ceo-also-apologizes-for-address-book-gate-calls-for-application-privacy-summit-guest-post/).

114. Indeed, copying address book data, photos and videos without a user's consent is against Apple's rules. Nevertheless, Apple failed to properly screen apps and allowed such apps to be sold in the App Store without disclosing to iDevice purchasers that their iDevices may be vulnerable to unauthorized access. Moreover, while Apple has removed apps that have violated its restrictions on pornography, Path continues to be available at the App Store.

115. This significant data breach has led two members of Congress to write to Apple's CEO to inquire about Apple's privacy problems:[12]

February 15, 2012

Mr. Tim Cook
Chief Executive Officer, Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
Dear Mr. Cook:

> Last week, independent iOS app developer Arun Thampi blogged about her discovery that the social networking app "Path" was accessing and collecting the contents of her iPhone address book without ever having asked for her consent. The information taken without her permission – or that of the individual contacts who own that information – included full names, phone numbers, and email addresses. Following media coverage of Mr. Thampi's discovery, Path's Co-Founder and CEO Dave Morin quickly apologized, promised to delete from Path's servers all data it had taken from its users' address books, and announced the release of a new version of Path that would prompt users to opt in to sharing their address book contacts.
>
> This incident raises questions about whether Apple's iOS app developer policies and practices may fall short when it comes to protecting the information of iPhone users and their contacts.
>
> The data management section of your iOS developer website states: "iOS has a comprehensive collection of tools and frameworks for storing, accessing, and sharing data. . . . iOS apps even have access to a device's global data such as contacts in the Address Book, and photos in the Photo Library." The app store review guidelines section states: "We review every app on the App Store based on a set of technical, content, and design criteria. This review criteria is now available to you in the App Store Review Guidelines." This same section indicates that the guidelines are available only to registered members of the iOS Developer Program. However, tech blogs following the Path controversy indicate that the iOS App Guidelines require apps to get a user's permission before "transmit[ting] data about a user".

[12] Internal footnotes omitted.

> In spite of this guidance, claims have been made that "there's a quiet understanding among many iOS app developers that it is acceptable to send a user's entire address book, without their permission, to remote servers and then store it for future reference. It's common practice, and many companies likely have your address book stored in their database." One blogger claims to have conducted a survey of developers of popular iOS apps and found that 13 of 15 had a "contacts database with millions of records" – with one claiming to have a database containing "Mark Zuckerberg's cell phone number, Larry Ellison's home phone number and Bill Gates' cell phone number."
>
> The fact that the previous version of Path was able to gain approval for distribution through the Apple iTunes Store despite taking the contents of users' address books without their permission suggests that there could be some truth to these claims.
>
> * * *

116. Apple did not adequately respond to the Representatives' letter, necessitating a March 14, 2012 follow-up:[13]

> March 14, 2012
>
> Mr. Tim Cook
> Chief Executive Officer, Apple Inc.
> 1 Infinite Loop
> Cupertino, CA 95014
>
> Dear Mr. Cook:
>
> We have received and reviewed the reply of Apple Inc., to our February 15, 2012, letter requesting information about your company's app developer policies and practices to protect the privacy and security of your mobile device users' information. We thank you for responding to our letter.
>
> The March 2 reply we received from Apple does not answer a number of the questions we raised about the company's efforts to protect the privacy and security of its mobile device users. In addition, subsequent to our letter, concerns have been raised about the manner in which apps can access photographs on your mobile devices and tools provided by Apple to consumers to prevent unwanted online tracking. To help us understand these issues, we request that you make available representatives to brief our staff on the Energy and Commerce Committee.
>
> * * *

117. On March 22, 2012, Representatives Waxman and Butterfield also sent letters to thirty-four sellers of apps inquiring about their information collection and use practices. These

[13] Internal footnotes omitted.

sellers included Foodspotting, Inc.; Synthetic, LLC (Disposable); Turntable.fm, Inc.; Twitter, Inc.; Foursquare Labs, Inc.; Quora, Inc.; Eye2i, Inc.(MusicPound); Tapbots, LLC (Tweetbot); Remixation (Showyou); Schematic Labs (Soundtracking); Massive Health, Inc.; Trover LLC; District Nerds, LLC; SoundCloud Ltd.; Hipster, Inc.; Forkley, Inc.; Tiny Review; Fashism, LLC; Path, Inc.; Banjo, Inc.; Redaranj, LLC (Recollect); Socialcam, Inc.; Brew Labs, Inc. (Pinterest); Piictu, Inc.; Stamped, Inc.; Burbn, Inc. (*Instagram*); Apple Inc.; Glancee, Inc.; d3i Ltd. (Momento); LinkedIn Corporation; SK Plante, Co., Ltd. (dishPal); and Facebook. The following letter to Lucas Buick, CEO of Synthetic, LLC is an example of these letters:[14]

March 22, 2012

Mr. Lucas Buick
Founder and Chief Executive Officer, Synthetic, LLC
d/b/a Disposable
74 Langton Street
San Francisco, CA 94103

Dear Mr. Buick:

> Last month, a developer of applications ("apps") for Apple's mobile devices discovered that the social networking app Path was accessing and collecting the contents of his iPhone address book without having asked for his consent. Following the reports about Path, developers and members of the press ran their own small-scale tests of the code for other popular apps for Apple's mobile devices to determine which were accessing address book information. Around this time, three other apps released new versions to include a prompt asking for users' consent before accessing the address book. In addition, concerns were subsequently raised about the manner in which apps can access photographs on Apple's mobile devices.

* * *

118. Similar concerns were raised by Senator Charles E. Schumer who called for a Federal Trade Commission investigation into the "disturbing and potentially unfair practices in the smartphone application market":

FOR IMMEDIATE RELEASE: March 5, 2012

SCHUMER CALLS FOR FTC INVESTIGATION OF APPLE AND ANDROID PHONE PLATFORMS THAT ALLOW APPS TO STEAL

[14] Internal footnotes omitted.

PRIVATE PHOTOS AND ADDRESS BOOKS AND POST THEM ONLINE – WITHOUT CONSUMER'S CONSENT

Reports Over the Last Week Revealed That Applications Developed for iPhones and Android Operating Systems Allow Third Party Access to Information Like Address Books and Private User Photos, Without User's Permission
Schumer Asks for Federal Trade Commission to Investigate and Determine if the Unauthorized Copying and Distribution of Private Information Stored on Cells Phones is an Unfair or Deceptive Practice

Schumer: When Someone Takes a Private Photo on their Private Phone, It Should be Just That: Private

United States Senator Charles E. Schumer today called for the Federal Trade Commission to launch an investigation into reports that smartphone applications sold on the Apple and Android platforms are allowed to steal private photos and customers address books. This past week, the New York Times revealed that iPhone and Android applications downloaded by users can actually gain access to a customer's private photo collection, and in some cases share the information online. This latest report comes on the heels of the discovery last month that applications on Apple devices like the iPhone and iPad were able to upload entire address books with names, phone numbers, and email address to their own servers. In both cases, users were not notified that their private information stored on their phone and or iPad could be copied and used by third party applications.

"When someone takes a private photo, on a private cell phone, it should remain just that: private," said Schumer. "Smartphone developers have an obligation to protect the private content of their users and not allow them to be veritable treasure troves of private, personal information that can then be uploaded and distributed without the consumer's consent."

According to reports by independent technologists, two separate loopholes, one in the Apple operating system and one in the Android operating system, allow apps to gather users' photos. In the case of Apple, if a user allows the application to use location data, which is used for GPS-based applications, they also allow access to the user's photo and video files that can be uploaded to outside servers. In the case of Android-based applications, the user only needs to allow the application to use Internet services as part of the app for third parties to gain access to photo albums.

"It sends shivers up the spine to think that one's personal photos, address book, and who-knows-what-else can be obtained and even posted online – without consent. If the technology exists to open the door to this kind of privacy invasion, then surely technology exists to close it, and that's exactly what must happen. The rapid innovation in technology, which is wonderful, must not also become an open invitation to violate people's privacy willy-nilly. When a consumer makes a private phone call or sends a letter the old fashioned way, they have a very reasonable expectation that the communication is private. The same standard must apply to our new technologies, too," continued Schumer.

Two weeks ago it was revealed that some of the most popular applications for smart phones were routinely collecting personal data from users' address books, despite policies in place from smartphone makers like Apple that explicitly prohibit such action without the prior consent of the user. After reports revealed this widespread practice, several applications announced they would end the practice. Questions remain, however, over the implementation of security policies employed

> by smartphone manufacturers and their oversight of applications sold on their platforms.
>
> Schumer today, in a letter to the Federal Trade Commission, called for the agency to launch a comprehensive investigation to explicitly determine whether copying or distributing personal information from smartphones, without a user's consent, constitutes an unfair or deceptive trade practice. Schumer is also urging the agency to require smart phone makers put in place safety measures to ensure third party applications are not able to violate a user's personal privacy by stealing photographs or data that the user did not consciously decide to make public.

119. THE NEW YORK TIMES technology columnist Nick Bolton likewise called out Apple's practices in a February 28, 2012 article entitled, "Apple Loophole Gives Developers Access to Photos":

> SAN FRANCISCO — The private photos on your phone may not be as private as you think.
>
> Developers of applications for Apple's mobile devices, along with Apple itself, came under scrutiny this month after reports that some apps were taking people's address book information without their knowledge.
>
> As it turns out, address books are not the only things up for grabs. Photos are also vulnerable. After a user allows an application on an iPhone, iPad or iPod Touch to have access to location information, the app can copy the user's entire photo library, without any further notification or warning, according to app developers.
>
> It is unclear whether any apps in Apple's App Store are illicitly copying user photos. Although Apple's rules do not specifically forbid photo copying, Apple says it screens all apps submitted to the store, a process that should catch nefarious behavior on the part of developers. But copying address book data was against Apple's rules, and the company approved many popular apps that collected that information.
>
> Apple did not respond to a request for comment.
>
> The first time an application wants to use location data, for mapping or any other purpose, Apple's devices ask the user for permission, noting in a pop-up message that approval "allows access to location information in photos and videos." When the devices save photo and video files, they typically include the coordinates of the place they were taken — creating another potential risk.
>
> "Conceivably, an app with access to location data could put together a history of where the user has been based on photo location," said David E. Chen, co-founder of Curio, a company that develops apps for iOS, Apple's mobile operating system. "The location history, as well as your photos and videos, could be uploaded to a server. Once the data is off of the iOS device, Apple has virtually no ability to monitor or limit its use."
>
> On Apple devices, full access to the photo library was first permitted in 2010 when Apple released the fourth version of iOS. The change was intended to make photo

> apps more efficient. Google declined to comment on how its Android operating system for mobile devices handles this issue.
>
> "It's very strange, because Apple is asking for location permission, but really what it is doing is accessing your entire photo library," said John Casasanta, owner of the successful iPhone app development studio Tap Tap Tap, which created the Camera+ app. "The message the user is being presented with is very, very unclear."
>
> The New York Times asked a developer, who asked not to be named because she worked for a popular app maker and did not want to involve her employer, to create a test application that collected photos and location information from an iPhone. When the test app, PhotoSpy, was opened, it asked for access to location data. Once this was granted, it began siphoning photos and their location data to a remote server. (The app was not submitted to the App Store.)
>
> The knowledge that this capability exists is not new, developers say, but it was assumed that Apple would ensure that apps that inappropriately exploited it did not make it into the App Store. Based on recent revelations, phone owners cannot be sure.
>
> "Apple has a tremendous responsibility as the gatekeeper to the App Store and the apps people put on their phone to police the apps," said David Jacobs, a fellow at the Electronic Privacy Information Center. "Apple and app makers should be making sure people understand what they are consenting to. It is pretty obvious that they aren't doing a good enough job of that."
>
> "We've seen celebrities and famous people have pictures leaked and disclosed in the past. There's every reason to think that if you make that easier to do, you'll see much more of it," Mr. Jacobs said. Not just celebrities are at risk, she added. "A lot of sites are trying to obtain images from everyday people and politicians to post online."
>
> As the Apple Store has grown to include more than 600,000 apps, and with Apple facing pressure from Google and Android, some worry that the company is becoming less vigilant about monitoring app developers, exposing users to unnecessary risks and shoddy apps.
>
> This month, Apple allowed a fake 99-cent Pokémon app into the App Store. Even though it offered only a series of Pokémon images, it became one of the most popular paid apps before it was removed by Apple.

120. After the filing of this lawsuit, on September 19, 2012, Apple released version 6 of its iOS. This iOS update included a Privacy setting that discloses what apps requested access to a user's Contacts app, Calendars app, Reminders app, Photos app, Bluetooth Sharing app, Twitter app and Facebook app. The Privacy function however does not show if any apps had in fact accessed the user's information and/or whether the third-party apps uploaded this information. Apple's decision to include this feature does demonstrate, however, that Apple has the ability

determine whether apps are accessing user data, despite representations that an "app can't access data from other apps."

Apple's Misrepresentations

121. Apple has represented to Plaintiffs and other purchasers, expressly or by implication, that the App Store does not permit apps that "violate[] [Apple's] developer guidelines including apps that violate user privacy."

122. Apple has represented to Plaintiffs and other purchasers, expressly or by implication, that: "Apple takes precautions – including administrative, technical, and physical measures – to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction." *See, e.g.*, Apple's customer privacy policy.

123. Apple has represented to Plaintiffs and other purchasers, expressly or by implication, that iDevices are "Safe and secure" and that "iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can't access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information…To guard your privacy, apps requesting location information must get your permission first." However, third-party apps such as Hipster and Path have admittedly accessed and uploaded users' full contacts information without user consent. Likewise, the iDevices are vulnerable to third-party apps uploading photos and videos when requesting access to user's location, despite Apple's promise that the iOS is secure and that apps cannot access data from other apps.

124. Plaintiffs and members of the Class relied upon Apple's representations with respect to the cost of their iDevices when making their purchasing decisions, and the omission of material facts to the contrary was an important factor in their decision.

125. For example, Plaintiff Pirozzi viewed the Apple website and saw in-store advertisements prior to purchasing her iPhone. She chose to upgrade from her Motorola Razor to the iPhone because she wanted a smartphone that had apps. The apps were an essential part of the

device for Plaintiff Pirozzi. Plaintiff Pirozzi keeps private photos and contact information of her family and friends on her iPhone. When Plaintiff Pirozzi purchased her iPhone she expected her contacts and photos not to be accessible to other apps. If Plaintiff Pirozzi knew that the apps would be able to potentially steal her private photos and contacts she would not have downloaded the apps and would not have paid as much for the iPhone, or would not have purchased the iPhone.

126. Likewise, each of the other Plaintiffs visited Apple's website, saw in-store advertisements, and/or was aware of Apple's representations regarding the safety and security of the iDevices prior to purchasing their own iDevices. Each such Plaintiff kept contact information in the Contacts App on their iDevice. When each such Plaintiff purchased their iDevice they expected their contacts not to be accessible to other apps.

127. Plaintiffs and members of the Class would not have purchased their iDevices and/or would not have paid as much for these devices if they knew the true nature of the iDevices.

ADDITIONAL ALLEGATIONS AGAINST APPLE

Apple and the App Defendants' Conduct

128. Despite marketing promises to the contrary, Apple sold Plaintiffs defective iDevices lacking promised features. Using the networked App Store, Apple and the App Defendants then infected Plaintiffs' iDevices with malware and computer contaminants designed to – and that did – take control of Plaintiffs' iDevices and unnoticeably relay Plaintiffs' valuable private mobile address books to the App Defendants via the Internet.

129. As a result, Plaintiffs' valuable private mobile address books were publicly exposed to numerous persons over the Internet and converted by the App Defendants for their own purposes and discretionary use.

130. More specifically, Apple sold Plaintiffs iDevices that repeatedly transmitted, broadcast and disseminated Plaintiffs' private mobile address books over the Internet and to unauthorized recipients without seeking or obtaining Plaintiffs' prior authorization to do so. According to Apple, Plaintiffs' iDevices were not supposed to do that. But, due to their defective

design, their lack of expressly promised security features, and Apple's and the App Defendants' knowing and complicit creation and deployment via the networked App Store of iDevice apps containing computer contaminants and undisclosed, hidden features onto Plaintiffs' iDevices in violation of Apple's own announced standards (and various industry standards and laws), they nevertheless did.

131. These unauthorized and unnoticeable mobile address book transmissions began after Apple deployed the App Defendants' identified apps to Plaintiffs' iDevices from the Apple App Store. Because the transmissions were not readily observable by Plaintiffs or detectible without technical prowess and additional equipment, Defendants managed to conceal the existence of these transmissions from Plaintiffs for some time. Defendants are aware of, but have continued to conceal when each App Defendant's identified app first included hidden computer contaminants containing instructions to trigger unauthorized mobile address book transmissions. These unauthorized transmissions, which crossed Wi-Fi, cellular networks, telephone lines and the Internet, continued until at least early February 2012.

132. These unauthorized transmissions contained substantial portions of Plaintiffs' mobile address books. For iDevices, the processor handles communications between the iDevice and the outside world. The processor separately handles and processes any communication calling up stored data or information. Thus, the transmissions consisted of contemporaneously intercepted, then relayed, iDevice processor I/O communications that had called up the Plaintiffs' mobile address books.

133. These transmissions (which Plaintiffs did not knowingly initiate) were ultimately relayed to and received by the App Defendants, which resulted in the App Defendants' obtaining substantial portions of Plaintiffs' mobile address book. Even though the App Defendants designed the computer contaminants hidden in their identified Apps to instruct iDevices to relay and transmit mobile address book information back to their own servers, the App Defendants are not legally intended recipients of those communications. Only the iDevice owners have the right and authority to select and designate the intended recipients of communications from their iDevices. Thus, the

unauthorized mobile address book transmissions obtained by the App Defendants amount to intercepted communications.

134. As a result, the App Defendants were able to electronically steal Plaintiffs' mobile address books using their iDevices. Plaintiffs were unaware that the App Defendants had, with Apple's knowing assistance, secretly obtained, retained and used their mobile address books.

135. These actions were contrary to the Defendants' express promises, marketing statements and warranties. Defendants each promised to respect iDevice owners' privacy, to protect iDevice owners' private information and to acquire and use only those materials consensually transmitted from owners' iDevices. App Defendants also promised that their apps would comply with Apple-mandated standards and all laws in any location where the app is made available and that their apps would not contain malware or surreptitiously access or disclose private user data. But they did.

136. Following a February 2012 NEW YORK TIMES investigative report, company officials at Defendants Foodspotting, Foursquare Labs, Hipster, Path, and Twitter publicly confirmed that their iDevice Apps were triggering unalerted mobile address book transmissions from their respective iDevice user bases and that their companies had received, used and stored iDevice owners' address books.

137. Apple agreed, concurrently announcing that:

> "Apps that collect or transmit a user's contact data without their prior permission are in violation of [Apple's] guidelines . . .."

138. Technical experts contemporaneously posted analyses, test results and reports identifying various Apps that uploaded and transmitted iDevice mobile address books without seeking the owners' prior permission, including these App Defendants' identified apps.

139. During the Class Period, Plaintiffs obtained the App Defendants' apps from Apple and unwittingly took those steps (for instance, they activated the App, navigated to certain screens, and/or tapped displayed buttons) needed to unwittingly trigger the unnoticeable transmission of their mobile address books. As a result, Plaintiffs' private mobile address books were transmitted

to the Internet, publicly disclosed and obtained, used, and kept by third parties, including these App Defendants.

140. By its statements and actions, including its supervision and governance of the iOS App Developer Program and the App Store, Apple voluntarily assumed a duty to protect iDevice owners from certain types of Apps, including those that (whether or not meant to by their principal designers) adversely impact iDevice owners' privacy. As exemplified by Apple's 2008 delisting of the *Aurora Feint* App, the 2009 delisting of the *Google Voice* App, and Apple's statements in its FCC Letter, Apple deems apps that relay iDevice owners' mobile address book to developers' (or third-party) servers without the iDevice owner's prior approval to be inappropriate for the App Store and for consumer iDevices.

141. Thus, as to those two apps, Apple adhered to (or at least appeared to attempt to adhere to and enforce for a time) its guidelines. But even in those two instances, Apple initially released and deployed the two apps on innumerable owners' iDevices before reversing course and later delisting each app.

142. Despite knowing that design flaws left iDevices' mobile address books insecure, Apple nevertheless helped the App Defendants deploy malicious apps containing these same harmful features to Plaintiffs' and Class Members' iDevices.

143. Not one of these Defendants alerted Plaintiffs or Class Members in advance to the fact that these apps would allow App Defendants to control and use their iDevices to surreptitiously take their private mobile address books. Apple never publicly recalled any of these apps. Nor did Apple remove these apps from the App Store or terminate their developers from the iOS App Developer program (as supposedly required).[15]

[15] Curiously, Apple did not hesitate in 2012 to remove BitDefender's *Clueful* App – which was designed to inform its users of the datasets that other apps installed on their iDevice silently accessed or transmitted – from the App Store. Apple also imposed a one-year ban on security researcher Charlie Miller when in late 2011, he intentionally passed a non-compliant app through Apple's review and onto the App Store in a proof-of-concept security test and reported to Apple the gaping security hole that he found in Apple's App procedures.

144. Thus, the App Defendants' identified apps contained computer contaminants within the meaning of California's Computer Crime Law, Cal. Pen. Code § 502, and met Apple's and other common published definitions for malware.

145. Apple also served and acted as each App Defendant's appointed agent with respect to marketing and deploying each App Defendant's app via the App Store and installing and activating each App Defendant's app on Plaintiffs' iDevices accordingly to its agreements.

146. The surreptitious iDevice mobile address book transmissions were, on information and belief, unencrypted and made over open wireless access (Wi-Fi) points (for instance, in coffee shops, restaurants, stores and businesses) as well as the Internet, turning Plaintiffs' iDevices into mobile beacons broadcasting and publicly exposing the unsuspecting Plaintiffs' mobile address books to numerous persons.

147. Defendants' actions had direct physical and use impacts on Plaintiffs' property. For instance, the unauthorized transmissions and operations used iDevice resources, battery life, energy and cellular time at a cost to Plaintiffs and caused loss of use and enjoyment of some portion of each iDevice's useful life. (iDevice batteries are depleted by use of the iDevice and require periodic recharging. Thus, these unauthorized transmissions and iDevice operations consumed electricity purchased by Plaintiffs.) The computer contaminants placed on Plaintiffs' iDevices also occupied each iDevice's limited memory space, which Plaintiffs paid for when purchasing their iDevices.

148. Plaintiffs' mobile address books and the contacts and materials therein are private. By their actions, each App Defendant (with Apple's direct participation) invaded Plaintiffs' privacy and intruded on their seclusion related to their private mobile address books.

149. The App Defendants (with Apple's direct participation) publicly exposed and de-privatized Plaintiffs' private mobile address books and the private materials contained therein. By doing so, they eliminated Plaintiffs' ability to solely control and keep that information private and unilaterally transformed those materials from ones that were private into unrestricted, non-private

materials that the App Defendants can seemingly keep, transfer and disclose to others in their own discretion.

150. As a result of Defendants' acts, Plaintiffs' private mobile address books were devalued and de-privatized and the App Defendants and Apple have impermissibly benefited by growing their user bases and networks exponentially, by gaining and retaining customers and by increasing sales.

151. Inconsistent with Plaintiffs' rights, the App Defendants and Apple by their actions exercised control over, converted, trespassed upon and deprived Plaintiffs of the intrinsic, extrinsic and commercial sales and rental/licensing value of both their iDevices and their mobile address books. Plaintiffs each had more than one hundred contacts in their iDevice mobile address books at all relevant times. Plaintiffs are each entitled to recover (i) the fair value of their iDevices (but in any event no less than a $10 daily market rental rate for each day that each an identified App exercised unauthorized control over a Plaintiffs' iDevice by executing an unauthorized address book transmission), and (ii) the fair value of their mobile address books, whether valued in the aggregate ($17,000 based on Harris Poll surveys) or on a per-contact basis (but in any event no less than a reasonable use or licensing fee – calculated either as a reasonable percentage of that intangible asset's value or $0.60 to $3.00 per contact according to industry reports) from each App Defendant who obtained, retained or used a Plaintiff's mobile address book or portions thereof and from Apple who helped them do so.

152. Apple could have, but chose not to, employ any one of a number of inexpensive, well known techniques to adequately secure iDevices and their Contacts databases and eliminate susceptibility to privacy-invading mobile address book harvesting functions like those employed in the identified apps.

153. Plaintiffs are entitled to have their iDevices repaired or modified to eliminate their susceptibility to similar future intrusions and to have the integrity their iDevices and data validated and repaired, as needed, and to have any vestige of these computer contaminants removed by an expert technician.

Apple's iDevices

154. The iDevices each feature a computer processor, on-device storage, a multi-touch interface (a touch-screen visual display), built-in Wi-Fi, wireless networking, and the ability to wirelessly receive from Apple and use aftermarket "Apps" that provide iDevice feature enhancements. Thus, each iDevice is also a hand-held computer.

155. Apps appear as icons on an iDevice's touch-screen visual display and activate and operate when the iDevice user touches displayed on-screen icons and buttons.

156. iDevices come with a written warranty and are accompanied by an iPhone or iOS software license ("iOS SLA"), which purports to license software accompanying the iDevice.

The iDevice "Contacts" feature

157. iDevices and the "Contacts" feature, by design, can take in from other sources the iDevice owner's existing off-device address book materials via wire, wirelessly and over the Internet. When connected to a designated computer or network, the iDevice syncs itself by communicating electronically with and transferring to the iDevice the owner's contacts and other materials from the computer or network.

158. Plaintiffs each synched their iDevices numerous times during the relevant time in which these Defendants were taking iDevice owners' private address book materials.

The Contact Address Book

159. A contact address book is a database within computing devices for storing entries called "contacts." Each contact consists of a few standard fields of data, including, but not limited to, contact names, e-mail addresses, instant message screen names, phone numbers, job employer, physical addresses, websites, birthdays, and notes.

160. The contact address book is one of the most private and personal files a user maintains on their iDevice. The contact address book reflects the connections, associations, and relationships that are unique to the owner of the iDevice. Not just which organizations the user belongs to, but which organizations the user actually communicates with on a regular basis. Is the user seeing a doctor? A psychiatrist? A specialist in the treatment of personal and potentially

embarrassing conditions? What political, social, or religious organizations is the user associated with? All of this information and more is revealed if an examiner can gain access to a user's contact address book. The contact address book answers a fundamental question with hard evidence: Who is this person communicating with?

161. iDevices come with pre-installed software permitting the user to enter certain categories of information related to the use of the iDevice. When the owner first receives the iDevice, all of the contact fields for the contact address book are blank.

162. In order to utilize the contact address book, the user must either have preexisting knowledge or must undertake some level of research, study, and self-learning in order to gain sufficient knowledge and skill to take advantage of the capabilities and parameters of the contact address book functions.

163. In addition, to utilize the contact address book, the user must individually mark, key-in, or input entries for each of the contact address book fields, utilizing the touch screen key pad on the iDevice, or they can import contacts that they created on their computer. Any creation of an address book would take at a minimum several seconds. Each individual entry requires time and investment of work and resources on the part of the user.

164. These choices of the individual, which are collectively incorporated into the totality of the contact address book in the iDevice, are highly personal and private. Contact address books are not shared, are not publicly available, are not publicly accessible, and are not ordinarily obtainable unless the user physically relinquishes custody of his or her iDevice to another individual.

165. The investment of time, effort, skill, and creative energy used to build the user's unique contact address book has independent value. The investment made by a user to create their contact address book is substantial and capable of valuation based upon the time spent learning and building the contact address book, the time spent creating and inputting data and information, the number of entries in the contact address book, and time spent modifying and updating the contact address book.

166. The cost to hire a technician to assemble the data and information contained in a contact address book is substantial. The technician would need to be familiar with iDevices (proficient in the use of the device), knowledgeable regarding the particular version of the contact address book supported by that particular iDevice, obtain the basic data and information from the user, and undertake the task of assembling and configuring the contact address book so that the final product fits the needs and desires of the user. These are skills that are available in the marketplace, but they would cost the user real dollars in order to employ a technician to undertake the task of creating or assembling the contact address book.

167. The contact address book is a product that has independent value in the marketplace. Companies that wish to obtain access to an individual's contact address book are ordinarily required to offer the user something of such value or use such that the individual is presented with a fair choice about whether to permit access to the contact address book in exchange for what is being offered. In such a case, the user is presented with a clear choice: in order to obtain the thing of value, the user will be required to provide the offering company access to the user's contact address book. Because information contained in the contact address book is ordinarily of such private and personal value to the user, the proposed exchange must ordinarily meet some minimum threshold of use or value to the user in order to persuade the user to open up their contact address book to the offering party.

168. The contact address book has independent value, not only to the user, but also to businesses engaged in profiting from and exploiting social media through advertising. The contact address book reveals not merely theoretical connections between people but the actual real-world connections that people engage in.

169. That information has independent value in the marketplace. For example, Facebook, the parent company of *Instagram*, has built a multi-billion dollar business based upon the personal, real-world connections between people.

170. Target marketing companies spend millions of dollars compiling information on the relational connections between people in their databases. The data they collect and compile is a commodity that they sell to businesses hoping to reach specific target audiences.

171. Lists of addresses, telephone numbers, and email addresses are commodities that are available for sale in the marketplace. Companies pay substantial sums for the right to market to a viable, verified list of current names, telephone numbers, and email addresses.

Apple's iAd Program

172. Since July 2010, Apple has delivered highly-targeted, location-specific, in-App ads to all iDevice owners under its *iAd* mobile advertising platform. iDevice owners cannot opt out of receiving these ads. Apple electronically gathers detailed demographic and usage information on every iDevice owner from his or her iDevice, which it uses for targeted *iAd* advertising and to pitch advertising clients to purchase *iAds* from Apple. Apple did not disclose to Plaintiffs that this would occur in advance of selling Plaintiffs their iDevices. Apple and its App developer Program registrants, including these App Defendants, split the revenues from these *iAds* 60/40.

The iDevice "App Store" App and Apple's App Store for Aftermarket Apps

173. Another built-in App on all iDevices is entitled the "App Store." The App Store app allows an iDevice owner to wirelessly browse for and obtain additional iDevice apps from Apple and to update apps already on the iDevice.

174. Apple also operates an off-device App Store, a centralized repository of apps available for iDevices combined with a digital app marketing, download, deployment and activation platform for promoting and wirelessly transmitting iDevice-compatible apps to every iDevice owner. All iDevices are tethered and networked to the App Store through their on-device App Store app.

175. The App Store is under Apple's exclusive domain and the Company has ultimate control of what apps are available to consumers. Furthermore, Apple has designed the iDevices to accept apps only from the App Store.

176. After Apple approves and provides a digital certificate for an App, Apple then markets, promotes, sells and deploys the App through the App Store, collecting all gross revenues and sales taxes. Apple retains 30% of the sales price of an App or any subsequent "digital goods" sold through an App and 60% of any additional future revenues from Apps that incorporate Apple's iAd advertising program. Apple pays any applicable state sales tax for an App sale (for both itself and the developer) based upon the stored account address it has for the recipient iDevice owner.

177. Apple contracts to serve as each Program registrant's agent for its App for these tasks. Nonetheless, Apple has previously told courts in this District that apps built by its Program registrants and listed on the App Store are Apple products, too.

178. Apple has direct and indirect monetary and business incentives to offer a wide selection of and deploy as many apps as possible – Apple makes money on and through them, even if they are initially "free."

179. By contracting to be a developers' agent on their apps, Apple placed itself in an inherently conflicted position and at odds with its iDevice owners, whom Apple had promised to protect from various types of harmful apps.

180. The App Store, which is run from California, affects and is involved in interstate commerce. For instance, businesses and individuals from all fifty states regularly communicate through the App Store both wirelessly and over the Internet. The App Store also regularly receives apps from and transmits apps to persons in all fifty states, both wirelessly and via the Internet.

The App Developer Program and Apple's discretionary control over the content, marketing, listing and deployment of Apps on the App Store

181. Just as Apple forces consumers to go through Apple to obtain Apps, Apple forces App creators to go exclusively through Apple, its App Developer Program, its testing, review and legal clearance process, its selection committee, its transaction processing system, and its App Store to get Apps to consumers' iDevices. These App Defendants and their identified Apps all went through these programs and Apple-mandated procedures.

182. Apple is thus the exclusive purchase, distribution and sales point for iDevice Apps and manages all administrative matters associated with App sales transactions. Apple establishes

and maintains the right to enforce legal and technical standards and policies and guidelines that Apps must meet and purports to review and test submitted Apps pre-release for compliance with those standards. Apple unilaterally decides which ones to offer to iDevice owners through the App Store.

183. Apple voluntarily chose to structure its iDevice App review and selection process this way. By comparison, Google-backed Android devices offer an open environment similar to an ordinary retail marketplace. Android device owners may obtain Android-compatible apps from whatever source makes them available, including directly from the creator of any particular app. Apple selected its "walled garden" model so that it could, according to Apple, exert full control over the content, selection, availability, and security of iDevice apps destined for its customers iDevices and "enhance the customer experience."

184. Apple completely controls users' experience from development of the iDevice, development and selection of the apps available on the App Store, as well as restriction of how the iDevice can be modified by users (e.g., such as blocking users from modifying their devices or installing unapproved software on their iDevices). Apple further restricts information concerning the development process and prohibits developers from publicly discussing Apple's standards for app development through the PLA.

185. The App Defendants each followed Apple's standard protocol for getting their identified Apps on the App Store.

186. Like anyone wishing to sell Apps via the App Store, and per Apple's mandate, they registered for the iOS Developer Program (the "Program"), paid Apple a $99 yearly program registration fee, and executed Apple's standard-form iPhone Developer Program License Agreement ("IDPLA").

187. The IDPLA is, in part, a license agreement authorizing program participants to use proprietary Apple software, code and tools – the same ones that Apple created and uses – to build iDevice Apps. Together, this Apple software (collectively known as the Apple iOS "Software Development Kit" or "SDK") and app developer Program resources provide Program participants

access to a wealth of information, tools, diagnostics and technical support services that Apple designed and published to facilitate and expedite the development of Apps for Apple's iDevice products.

188. The resources Apple provides to Program participants include editing software, simulators, forums, guides, design and approval criteria, code, code resources and libraries, APIs, performance enhancing tools, testing software, and mentoring via access to Apple engineers who "provide … code-level assistance, helpful guidance, [and] point [the developer] towards the appropriate technical documentation to fast-track [his/her] development process."

189. Thus, developers do not start from scratch; Apple provides Program registrants all the pieces and components pre-built they need to build iDevice Apps. As a result, all iDevice Apps were built, in part, by Apple.

190. Despite Apple's public statements that it protects its iDevice owners' privacy, Apple's Program tutorials and developer sites conversely teach Program registrants how to code and build apps that non-consensually access, manipulate, alter, use and upload the mobile address books maintained on Apple iDevices – precisely what these App Defendants' identified apps did. As Program registrants, the App Defendants were exposed to and aware of these tutorials and developer sites and, on information and belief, their personnel utilized them to build the identified apps.

191. The App Store Review Guidelines set forth the technical, design, and content guidelines Apple will use when reviewing an app for inclusion in Apple's App Store. These guidelines state that apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." This includes the transmission of personally identifiable information. In addition, the requirements of the PLA empower users to control access to user or device data, and require user consent before user or device data can be collected.

192. Apple also requires each Program registrant to re-submit his or her app for another round of testing and compliance verification whenever a change, update or new version is built.

193. Apple retains the unilateral, discretionary authority to terminate sales, listing, promotion or deployment of any app and/or terminate the Program account of any app developer for non-compliance with Apple's development policies and standards. Further cultivating its security-conscious image, former Apple CEO Steve Jobs also publicly touted in interviews that Apple had a built in "kill switch" (either in the iDevices or the apps) that it could use to remotely disable already-issued Apps if Apple learned post-release that an app was non-compliant. It is unclear, though, whether Mr. Jobs' statement was true or not.

194. Apple reviewed each new and updated version of the App Defendants' identified Apps. Though they repeatedly contained computer contaminants to secretly relay iDevices' mobile address books in violation of Apple's policies and standards, Apple listed them and offered and deployed the Apps over the App Store. Apple never removed them from the App Store, never exercised its right to terminate the developer's participation in the Program, and never activated Mr. Jobs' dreaded "kill switch."

195. The Program, which is run from California, affects and is involved in interstate commerce. For instance, businesses and individuals from all fifty states and internationally regularly communicate through and with the Program via the Internet. Apple, via the Program, also regularly receives via the Internet Apps submitted from around the world.

196. Each App Defendant has communicated with or through the Program, associated with Apple through the Program, and submitted its Apps to Apple through the Program.

197. The developers of the *Foodspotting, Foursquare, Hipster, Kik Messenger, Path, and Twitter* apps have confirmed publicly that each of their apps caused users' iDevices to relay users' mobile address books to their company servers.

Standards and Duties of Care

198. Apple and the App Defendants are subject to standards and duties of care established by Apple, by the industry and by law. Affirmative duties include selling non-defective iDevices; accurately representing iDevice features; building, offering, selling, or deploying apps that do not contain malware or computer contaminants, take or use iDevice owners' property

(iDevices or mobile address books), expose iDevice owners' private information (mobile address books or their contents), or enable others to do so.

199. Apple, Google and Amazon.com operate the three largest wireless mobile device app marketplaces and have established consistent standards that they disclose to developers.

200. Google and Amazon.com list and sell Android mobile devices apps. Both mandate that apps must: (i) comply with all applicable laws; (ii) protect user privacy and private information; and (iii) notify users in advance and obtain user permission prior to accessing or transferring personal or private information or property from the user's device. Amazon.com also prohibits apps that "have the potential to infringe upon an individual's privacy."

201. The App Defendants must abide by standards specified in Apple's Program terms, standards, documentation, guides, guidelines (including Apple's App Store Review Guidelines) and agreements (including Apple's IDPLA and SDK agreements). These materials are publicly available. Apple does not keep confidential its IDPLA and SDK agreements, which are available online and in company SEC financial reports and which Apple sent to almost a million of recipients.

202. Apple builds and releases iDevice Apps and is subject to all standards it mandates on others pertaining to creation, release or deployment of Apps via the App Store. Apple must also comply with all standards established by its public statements (including those made in Apple's marketing and promotional literature, media statements, product launches, seminar presentations, executive interviews, keynote addresses and to government agencies).

203. Based on its conduct and statements, Apple voluntarily assumed duties to (i) adequately analyze, test and review apps for reasonably foreseeable dangers before deploying them to owners' iDevices; (ii) adequately warn of any hidden, malicious or potentially privacy-invading features in an app; (iii) not release Apps that transfer users' private mobile address books without seeking explicit consent; and (iv) build adequate security features into iDevices.

204. Apple's App Store Review Guidelines mandate that: (i) private data not be obtained from an iDevice without owner consent; (ii) apps not have secret hidden features; and (iii) apps

comply with local legal requirements in all jurisdictions in which the app is available (subjecting each to the highest applicable legal standard). Each App Defendants' identified app was available in all fifty states and, on information and belief, in Europe and is subject to heightened EU statutory privacy measures.

205. Apple mandates that iDevice owners' mobile address books must be afforded property protections, instructing all developer Program registrants that "***the Address Book database is ultimately owned by the user***."

206. Apple's IDPLA and SDK agreements mandate that developer Program registrants' Apps not "scrape" data from iDevices absent express prior consent. Further, per Apple's FCC Letter:

> "Apple provides explicit language in its agreement with iPhone developers regarding prohibited categories of applications, for example:
>
> > 'Applications may be rejected if they contain content or materials of any kind (text, graphics, images, photographs, sounds, etc.) that in Apple's reasonable judgment may be found objectionable, for example, materials that may be considered obscene, pornographic, or defamatory; and
> >
> > Applications must not contain any malware, malicious or harmful code, program, or other internal component (e.g. computer viruses, trojan horses, 'backdoors') which could damage, destroy, or adversely affect other software, firmware, hardware, data, systems, services, or networks.'"

207. Apple CEO Steve Jobs publicly characterized a malicious application as one that takes users' personal information without seeking or obtaining prior permission. Industry definitions for malware are consistent with Apple's, which it makes available to developers:

> **What is malware?**
>
> ***
>
> Malware is an abbreviated term for malicious software. Malware includes viruses, worms, trojan horses, and other types of software that can damage your system or *violate your privacy*. Malware can be installed on your computer when you download content or applications from the Internet, either from email or websites.
>
> Certain instances of malware are merely harmless or annoying. More often, its intent is to take control of your computer to collect personal information, host illegal content, send spam email, or cause harm to other systems on the network. Personal

> information that's collected often includes credit card, banking accounts, social security numbers, or other identifying information leading to identity theft and financial loss.
>
> Avoid opening items downloaded from websites and email messages unless you are certain that they come from a legitimate, trusted source. If you are uncertain about the source of a downloaded item, it is best to delete the item. You can always download it again later, after you have made certain that the item is not malware.
>
> *See* Apple publication at
>
> http://docs.info.apple.com/article.html?path=Mac/10.6/en/27449.html

Apple Representations

208. Apple made numerous representations and assurances to Plaintiffs, Class Members and consumers in advance of their purchase of iDevices and in advance of their receipt from Apple of the App Defendants' identified apps. Apple made these representations and assurances to encourage Plaintiffs and Class Members to purchase iDevices and accept add-on apps from the App Store.

209. Apple also assured consumers that for data-security purposes, "Applications on the device are 'sandboxed' so they cannot access data stored by other applications." Apple, in its iDevice literature, identifies the "Contacts" feature as such an "application." Nevertheless, iDevice contacts and the iDevice "Contacts" database were not sandboxed. Instead, they were accessible to, alterable by and transmittable by every App on the iDevice. Apple seemingly admits that is so in its FCC Letter. Consequently, contrary to Apple's assurances, Plaintiffs' private mobile address books were accessible to, alterable by and transmittable by every App that came with or that Plaintiffs' subsequently added to their iDevices, including the App Defendants' identified Apps. Apple never warned Plaintiffs of this.

210. Apple's statements were part of the basis of the bargain under which consumers, including Plaintiffs, purchased their iDevices and accepted App Store apps. These Apple statements constitute and are express warranties. Apple is strictly liable to Plaintiffs for breaching these express warranties and for failing to warn Plaintiffs either that these statements were inaccurate or about the reasonably foreseeable risks and harms that Plaintiffs in actuality faced relating to their iDevices, their privacy and their private mobile address books using their iDevices

as intended or accepting Apps (and in particular, the App Defendants' by Apps) from the App Store.

211. From 2008 to the present, the highest levels of Apple (from its founder to its current CEO to its corporate spokespersons) have so consistently expressed publicly that Apple protects its customers' and iDevice owners' security and privacy that – though inaccurate – it is ingrained into the image of Apple's culture, products and offerings as well as in the minds of customers. Apple has never corrected this falsity or misimpression. (In actuality, Apple is instead one of the largest data aggregators on the planet, having amassed via the App Store and iTunes Store a database of hundreds of millions of consumer names, addresses, email addresses, credit card numbers, location dataset and personal demographic information, which it leverages daily through its iAd targeted advertising program.)

Apple Guidance Perversely Encourages Data Theft

212. Apple contractually required developer Program registrants to abide by its *iOS Human Interface Guidelines* reference manual included in Apple's iOS DEVELOPER LIBRARY, which in part stated:

- at p. 47: "Get information from iOS, when appropriate. People store lots of information on their devices. When it makes sense***, don't force people to give you information you can easily find for yourself, such as their contacts*** or calendar information."
- at p 48: "***iOS devices are personal devices***, but they also encourage collaboration and sharing with others. Enhance your app by helping people collaborate and connect with others. When appropriate, ***make it easy for people to interact with others and share things*** like their location, opinions, and high score .... ***People generally expect to be able to share information that's important to them***."
- at p. 63: "It's often said that ***people spend no more than a minute or two evaluating a new app. ... Avoid displaying an About window or a splash screen***. In general, try to ***avoid providing any type of startup experience that prevents people from using your application immediately. Delay a login requirement for long as possible***. Ideally, users should be able to navigate through much of your app and understand what they can do with it before logging in."
- at p.65: "If possible, ***avoid requiring users to indicate their agreement to your EULA when they first start your application.*** Without an agreement displayed, users can enjoy your application without delay."

213. In direct conflict with the customer assurances and standards it espouses and purportedly mandates, Apple's *iOS Human Interface Guidelines* manual teaches and suggests Program registrants design and build Apps that: (a) directly and automatically access contact data – particularly whenever the developer may desire it for collaborative or sharing purposes – without any prior alert(s) to the app user; and (b) download, operate, and function in advance of any presentation of or user consent to an End User License Agreement ("EULA") or privacy policy. In accord with Apple's instructions, the App Defendants to Plaintiffs' recollection did not present either an EULA, terms of service, privacy policies or any other terms to Plaintiffs in advance of the download, installation, activation and initial operation on Plaintiffs' respective iDevices of each App Defendants' respective App.

214. Consequently, despite supposedly mandating that Program registrants' Apps not include malicious, surreptitious or privacy-invading data harvesting functionalities (and supposedly reviewing and testing all Apps to ensure the absence of forbidden functionalities), Apple taught Program registrants' to incorporate forbidden data harvesting functionalities – even for private "contacts" – into their Apps and encouraged Program registrants to design those functions to operate in non-discernible manners that would not be noticed by the iDevice owner. These App Defendants, apparently in accord with Apple's instructions, did just that with their identified Apps.

Undisclosed Material Information

215. Apple never disclosed to Plaintiffs that their iDevices would or could (either alone or in combination with an App) self-transmit the iDevice address book without user input or authorization from the iDevice owner.

216. Apple, however, knew of this security hole and of episodic, App-initiated exploitations of this iDevice flaw for quite some time. For instance, Apple knew that Program registrants' Aurora Feint and Google Voice Apps exploited that security hole in 2008 and 2009 and was also informed by a team of scientists and the media in 2010 that the *Gowalla* and Kik Messenger Apps did so too. Apple still has not warned or notified iDevice owners of this flaw or of the risks associated with this flaw.

217. Apple never disclosed to the Plaintiffs that the "Contacts" feature and its Contacts database (the mobile address book) was not "sandboxed" and lacked promised security protections.

218. The App Defendants did not disclose to Plaintiffs in advance of Plaintiffs obtaining the identified Apps that installation or use of those Apps on their iDevices could or would cause the iDevice to self-transmit the iDevice owner's private mobile address book without owner input or prior authorization. Apple did not inform Plaintiffs of these facts, either, though it reasonably should have been aware of these facts from its testing and review of each App.

Aurora Feint

219. After releasing the Aurora Feint App to the App Store and downloading and deploying the App hundreds of thousands of consumers' iDevices, Apple delisted the App when media reports from July 2008 revealed it to be transmitting iDevice owners' contacts database to the developer's servers without asking if it could do so.

220. Previously Aurora Feint soared to the top of the App Store's popularity list, (presumably due its automated address-book-harvesting and consequent networking-fueled viral growth).

221. Somehow, that non-compliant App made it past Apple's supposed "comprehensive" and "rigorous" testing and review process.

222. This occurred just a few weeks after Apple first launched the App Store.

223. After a three-day ban from the App Store, it returned with Apple's approval (but this time missing the malicious portion that caused Apple to pull it). Again Apple even promoted the re-released Aurora Feint App on its What We're Playing App Store list despite the developer having just flaunted Apple's policies and disrespected user's privacy..

224. Apple was thus immediately aware within weeks of launching the App Store that its iDevices had – and that App developers were inclined to exploit in order to gain private mobile address books' contacts data – security flaws directly associated with the iDevice mobile address book.

225. Apple immediately knew, too that consumers' mobile address books – themselves both a network (the owner's "social graph,") and a listing of network contact points (i.e., the email, phone and other contact points for everyone in that iDevice owners' address book – could be readily mined, exploited, and used by App developers to fuel viral app user-base growth and were a desired commodity desired and in high demand by App developers (regardless of whether Apple's policies indicated that those materials were off-limits or subject to owners' superior privacy and property rights).

Google Voice

226. After initially releasing the Google Voice App to the App Store and downloading and deploying the App to a substantial numbers of consumers' iDevices in 2009, Apple delisted that App after four months.

227. Apple states in its FCC Letter that its rationale for that decision: "the iPhone user's entire Contacts database is transferred to Google's servers, and we [Apple] have yet to obtain any assurances from Google that this data will only be used in appropriate ways." (Apple does not explain in its FCC Letter, though why it chose to initially release the non-compliant Google Voice App in the first place.)

228. Per Apple's FCC Letter, Apple was capable by 2009 of discerning whether an App had the capacity to transfer the iDevice's Contacts database to the developer's servers.

229. Where an App contained a function that could transfer the iDevice's Contacts database to the developer's servers, per Apple's FCC Letter, Apple supposedly required additional "assurances [from the developer] that this data will only be used in appropriate ways." (Apple does not explain in its FCC Letter though, what is meant by "appropriate ways" or why Apple, rather than the owner of the address book, should have final say what uses of that owner's data are "appropriate.")

230. Thus, early on in the life of the App Store, Apple established a pattern of first releasing an App (despite apparent privacy and address book-related problems that Apple knew or should have known about), then delisting it months later if negative media reports surfaced.

ALLEGATIONS REGARDING SPECIFIC APP DEFENDANTS

Gowalla

231. App Defendant *Gowalla* built the *Gowalla* App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the *Gowalla* App on the App Store and served as *Gowalla*'s world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

232. In 2010, a team of professors and doctoral computer science candidates determined that the *Gowalla* App was, without prior permission, uploading and transmitting iDevice address book materials – mainly fields of names and corresponding email addresses – in their entirety to the developer when users viewed their contacts through the App.

233. The scientists sent Apple a "detailed report" on what the *Gowalla* App was doing through Apple's designated channels for problem reporting, even providing screen shots of the App's unencrypted address book transmissions. (The scientist later reported about this in a peer-reviewed paper.)

234. Apple ignored the gist of their report, stating back to them, "If you have a privacy concern, you should contact the developer." With that, Apple apparently washed its hands of the matter.

235. The *Gowalla* App remained available on the App Store to iDevice owners for more than a year after that, until its successor (Facebook) eventually shut it down.

236. Plaintiffs Beurhausen, Dean, King, Mandaywalla, Paul Sandiford and Varner (the "*Gowalla* Plaintiffs") each recall using the *Gowalla* App, logging in and navigating within the App to a "Find Friends" menu screen and being offered various options (including an option entitled "Address Book").

237. The *Gowalla* Plaintiffs do not recall being presented at any time with an intervening alert or display indicating that the *Gowalla* App would transmit his or her mobile address book to *Gowalla* (or anyone else) or warning that such a transmission was about to occur.

238. On information and belief, by that point (before the user made any menu selection on the "Find Friends" screen) the *Gowalla* App had already relayed the *Gowalla* Plaintffs' mobile address books to *Gowalla*'s servers, without first asking for or securing consent.

239. As a consequence, *Gowalla* obtained and was able to retain, keep, remotely store, and use at its discretion Plaintiffs' private address book materials.

240. The *Gowalla* App never requested permission to upload, transmit, or disseminate any portion of Plaintiffs' iDevice address book materials. Nor did *Gowalla*.

Kik Messenger

241. Plaintiffs Dennis-Cooley and Green (the "Kik Plaintiffs") each recall using the Kik Messenger App, logging in and navigating within the app.

242. App Defendant Kik Interactive built the Kik Messenger App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), in late 2010 Apple released, promoted and deployed the Kik Messenger App on the App Store and served as Kik Interactive's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

243. Three weeks after its release, the Kik Messenger App suddenly had over two million users.

244. According to Kik Interactive personnel, the "secret sauce" for Kik Messenger's eye-popping, viral growth was that the App relayed every email address contained in each new user's wireless mobile device's address book to Kik Interactive's servers, which Kik Interactive then followed with an immediate "push" notification to both the device owner and any matching email contact found in Kik Interactive's database. According to Kik Interactive, this all occurred

automatically and without warning upon installation of the Kik Messenger App. Basically, Kik Interactive took and spammed the device owner's entire address book.

245. Kik Interactive thus wrongfully obtained, retained, disclosed and de-privatized the identified Plaintiffs' valuable private address books and used their iDevices without authorization. At the time, Kik Interactive and its App never asked Plaintiffs in advance if they could do any of these things.

246. Apple knew this was transpiring. Kik Messenger's viral growth taxed Apple servers. Plus, reporters wrote up numerous reports with titles like, "Speedy Messenging App Kik Goes Viral, But is It Cool With Apple's T[erms]O[f]S[ervice]?" and contacted Apple for answers to the question that article posited. Apple chose not to comment or warn consumers.

Path

247. App Defendant Path built the Path App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted, and deployed the Path App on the App Store and served as Path's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

248. Path—launched in November 2010—operates an online business as a smartphone-based social network utilizing an application software that performs specific functions for a web-based platform on mobile devices. Path describes its business as: "A smart journal that helps you share life with the ones you love" in a "trusted, intimate environment."

249. Apple is a joint-venturer in the iFund venture capital fund and mentoring program ("iFund") with the venture capital company Kleiner Perkins. Path is an iFund company. On information and belief, Apple owns a portion of the iFund and provided mentoring to iFund-financed companies (including Path) and the iFund owns or owned a portion of Path's equity. On information and belief, Apple provided direct guidance, assistance and mentoring to Path on its Path App.

250. Path's launch App, "Path v.1," initially allowed its users to post photos and add tags for people, places, and things. While not a technologically innovative concept for Apps, there was an added limitation that users could only include fifty connections, which was a marketing innovation. This limitation related to a marketing plan to promote a corporate philosophy to create a more authentic experience with the user's closest friends instead of trying to "make the world a more open place," which is another social network's motto.

251. Path's business model appeared to the mobile App industry to be anti-social, not lending itself to viral levels of user adoption, lacking "robust" features, and doomed to failure. However, a few "insiders," such as Google, which reportedly offered $100 million to purchase this new startup, understood the viral implications revealed in Path's provisional applications. While Path's business model is different, its business plan is the same as most App developers interested in profits: provide a nominal service to attract users with the common objective to obtain and sell user data. An App's existence and prospects for funding by venture capitalists ("VCs") is often premised upon user data acquisition, since user data is a "commodity" for sale. The dilemma for App developers is how to obtain substantial amounts of user data without a user's knowledge. It is well known that users who are asked to opt-in to provide personal info will not agree to such due to privacy concerns. Such hesitation will ultimately cause users not to provide data, which will terminate or limit VC funding, and the Apps would cease to exist.

252. In March 2011, Path activated its integration function in "Path v.1.5" for online social networks so that its "Friend Rank" algorithm could follow its users from the Path App to the users' other social networking platforms. Without such functionality, Path was unable to expand since its users could not "push" content from Path to social networks such as Facebook. This integration function was necessary for Path's plan for data collection of its users' "interactions" with contacts while in third-party on-line social networks.

253. In November 2011, Path re-launched as "Path v.2.0," incorporating a set of activities—Photos, People, Places, Music, Thoughts, and Sleep/Awake status—that users could post to their timeline and share with their network. By initially focusing on these social services,

Path's mobile functionality could now compete with the most popular mobile Apps available, including functions such as:

- photos incorporating image-filters;
- a check-in service to allow location data to be posted;
- an ability to insert song clips into a user's timeline; and
- allowing users to post comments to be shared to both a user's Facebook and Twitter accounts.

254. Path consistently marketed itself to Plaintiffs and iDevice owners as focused on protecting App users' privacy.

255. Path stated on company websites touting its App that, "Path upholds the expectations for privacy of both the mobile phone and the journal with its limited, intimate, more personal network."

256. Path founder and CEO Dave Morin stated in 2010 to a technology reporter that, "Path does not retain or store any of [the user's] information in any way."

257. Path also publicly announced that its App was "private by default" and said users "should always be in control of [their] information and experience.'" Morin reiterated in 2011, that the Path App is "private by default and always will be."

258. These representations and statements were knowingly false, but Path and Morin never corrected them before February 2012.

259. In actuality, Path had been taking, using and storing iDevice owners' mobile address books without permission or notice, including those of the identified Plaintiffs (each of whom had earlier obtained and activated the App).

260. After Apple downloaded the Path App to the Plaintiffs' iDevices, Plaintiffs Carter, Dennis-Cooley, Green, and Paul (the "Path Plaintiffs"), each recalls opening the Path App, signing up via a "Sign Up" screen, and using and navigating around the App.

261. The Path Plaintiffs were never told beforehand that Path's App could or would cause their iDevices to, without notification or permission, transmit and upload their private mobile address books or that Path would obtain and remotely retain and use them.

262. However, according to news reports, when the Path App was deployed on an iDevice and the user registered for an account, the Path App automatically—without any additional notification to or input from the user—called up the iDevice's address book, made the Internet call "https://api.path.com/3/contacts/add" from the iDevice, then wirelessly uploaded and transmitted to Path's company servers in a ".plist" the complete set of names, phone numbers, email addresses and even physical addresses maintained in the user's iDevice's mobile address book.

263. At no point before February 6, 2012 did Path ever ask Plaintiffs if they could do any of these things.

264. Plaintiffs recall no warning or notice from Path or its App, and did not consent to Path's surreptitious conduct. (In contrast the Android version of the Path App alerted its users.)

265. On information and belief, Plaintiffs' address book materials were not relayed in a reasonably secure manner from Plaintiffs' iDevices by Path's App or stored in a reasonably secure manner on Path's servers.

266. Path knowingly and intentionally accessed, uploaded, transmitted to its servers, used, and remotely stored its users' private mobile address books maintained on their iDevices, including Plaintiffs' and Class Members. By doing so, Path obtained, retained, disclosed and de-privatized the identified Plaintiffs' valuable private mobile address books and used their iDevices without seeking (or obtaining) authorization to do so. At the time, Path and its app never asked Plaintiffs in advance if they could do any of these things.

267. On information and belief, these actions re-occurred when Plaintiffs and other Path users re-launched or updated the Path app, which Plaintiffs regularly did up through February 6, 2012.

268. Path's collection and storage of user address books violated Path's policies and Apple's guidelines.

269. On February 8, 2012, Path issued and Apple released on the App Store a revised versions of the *Path* app, which then included the following new opt-in alert:

> "**Contacts** To find family and friends, Path needs to send your contacts to our server" [Don't allow] [OK]"

270. Path conceded at that time that an opt-in alert and notification screen was needed before the upload of any user address book materials to protect user privacy. However, the revised *Path* App still did not cryptographically hash address book data before those upload.

271. Around April 2, 2012, Path announced that its app would begin "hashing user contact data" to, it asserted, "protect user privacy." Cryptographic hashing is a free, well-known, commonly-used technique long known in the industry that is commonly used to securely and privately anonymizes private data for matching purposes.

272. Due to the well-publicized nature of Path's activities, on February 15, 2012, House Energy & Commerce Chairman Henry Waxman sent a letter to Apple requesting information following complaints that some smartphone Apps were accessing and retaining users' contact data without permission. The inquiry requested documentation revealing that its investigation would focus on Apps that read ("sniff") a user's contact address book upon initial activation, without notice or authorization, ostensibly to locate user's "friends" within the App. The impetus for this inquiry by Representative Waxman originated when a researcher discovered Path's unauthorized access to, and retention of, its users' contact address book data. However, attention was quickly diverted to the entire App industry when Path's CEO David B. Morin claimed that this was a "common practice." With attention diverted away from Path, and an inquiry initiated against an entire industry's "common practice," Path's "uncommon practices" as to how it used the contact address data were ignored and attention was not given to an analysis of its provisional application number 61/363,081, filed on July 9, 2010, entitled "System and Method for Social Interaction with Geolocation and Automated Aging and Pruning of Interactions and Contacts."

273. The underlying purpose for the Path App was data mining of mobile devices to obtain PII, as opposed to a platform for content aggregation. This provided the ability to eliminate substantial server costs and allowed access to user content that provided tracking data and an immediate established platform.

274. Aggregation of users' data as content evolved over time, from methods used by search engines evolving from being operating systems, to only aggregate content, to actual content

creation. Search engines then progressed to re-aggregating the content until socially-oriented sites provided a forum for their users to create the content. As Apps first emerged, online social networks sought to aggregate user data within their own social network platform, thus controlling the user engagement within the social network. An example of this are Apps made by Zynga within the Facebook Platform. As App development exploded in 2008, Apple, and then Google in its Android market, sought to create a platform for Apps independent of a social network platform. However, there remained no available platform for App developers to draw a social context from data available in a social network platform. Facebook Platform Connect sought to provide a system and method to remedy this dilemma, by providing a platform that permitted access to its social network that allowed a social context to Apps that were external to Facebook. However, the social networks provide only limited information and do not offer a social context to the App. That is, a user of the third-party App could not see what other users of the social network were doing or access information about other users of the social network that was not publicly available.

275. Facebook Platform Connect provided a system and method for providing a social context to software Apps. A user of a social network could authorize access by an external software App to information available in the social network. When the users of the social network use the external App, the App contacts the social network provider for permission to access the information available in the social network. If access has been authorized, the App incorporates the information from the social network into its interaction with the user, providing a social context to the user's interaction with the App.

276. Facebook Platform Connect also provided a platform for using a social network to provide a social context to a software App that was external to the social network, such as an App developed by third-party developers like Path, rather than the social network provider, and which did not reside within the social network or social network provider. A social context comprises information that personalizes the interaction of a user with the software App. Installation did not require the user to download the App onto their mobile device and enabled the user to interact directly with the App while the App itself remains on another device. Installation could also allow

the App to access information about the user that was available through the social network platform.

277. A certain design point of the Path App architecture are the icons on the screen page which reveal functions that involve digital content, user content, GPS location information, and network access. The design is a simple but effective way to provide the mechanisms required for substantial user data collection and an ability to "turn on" the device for data collection and monitoring without the user's involvement. Path's ability to have continuous network access to the users' device is marketed to the public as a service to notify users' friends if the user is asleep or awake by the use/non-use of the mobile device.

278. Path's designs also are streamlined to expedite users' access and use of its core functions. Online social networks, such as Facebook, provide barriers to users since there are multiple screens required to be accessed before they can upload digital content. With the advent of mobile Apps, users are gravitating towards platforms that have more speed and simplicity for uploads, such as Path.

279. By December 2011, Path's membership had grown from 30,000 to over 300,000 in less than a month:

> In the two months since Path [version] 2 launched, it has attracted a million new users, according to Path CEO Dave Morin. That's roughly the same amount Path got in its entire first year. . . .
>
> Path users have created over 50 million items of content and half a billion pieces of feedback. The latter is a somewhat inflated stat, because "feedback" is created every time a user looks at content on Path. But for reference, there are 15 million pieces of feedback created on Path per day now, versus 10 million total in the first year, Morin said.[16]

280. While Path heralded its success, there was no explanation provided for Path's miraculous rapid growth, increasing its user base tenfold within just one month. A researcher's findings four months later would provide insight into the reasons for such success.

---

16 Liz Gannes, *Path Now Has 2M Users, Having Doubled Since It Relaunched Two Months Ago*, AllThingsD (Feb. 3, 2012), http://allthingsd.com/20120203/path-now-has-2m-users-having-doubled-since-it-relaunched-two-months-ago/.

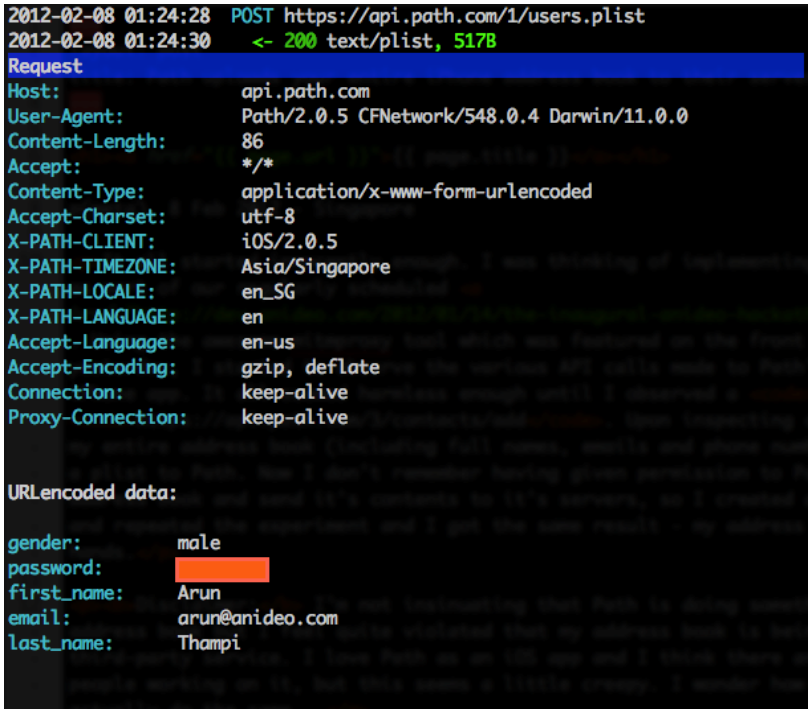
281. On or about February 8, 2013, Path entered into a Consent Decree with the United States Department of Justice enjoining it from, *inter alia*, continuing to misrepresent to consumers the extent to which it maintains and protects the privacy and confidentiality of information stored on iDevices, including contact information.

Thampi Study—Path's Deceptive Practices Revealed

282. On February 8, 2012, Arun Thampi discovered that Path was uploading its users' entire contact address books to its servers.

283. Thampi's discovery was made by using a software tool called mitmproxy, which relies on a common methodology referred to as the "man-in-the-middle," which analyzes data sent to and from an App in real time. The findings were reported as follows:

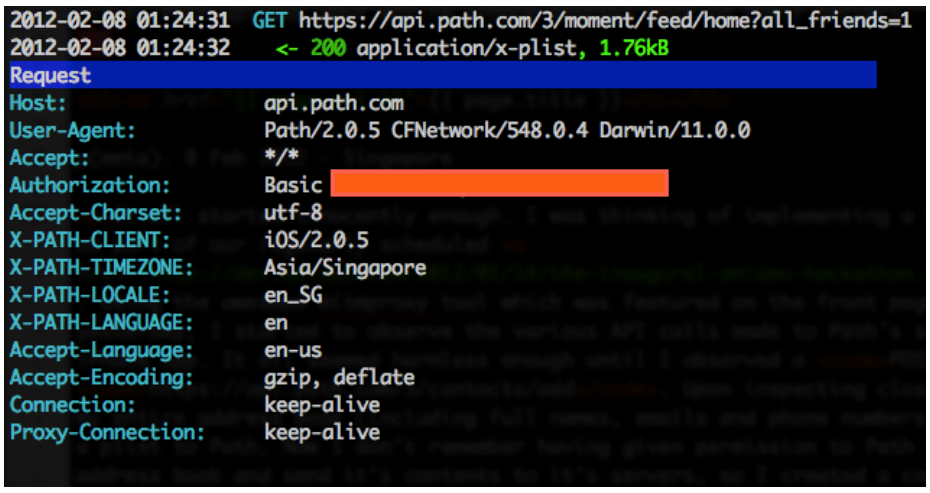
> I noticed that my entire address book (including full names, emails and phone numbers) was being sent as a plist to Path. Now I don't remember having given permission to Path to access my address book and send its contents to its servers, so I created a completely new "Path" and repeated the experiment and I got the same result – my address book was in Path's hands. . . .
>
> The Trail of Events
>
> 1. https://api.path.com/1/users.plist
>
> As soon as you create a new account to Path, a call is made to https://api.path.com/1/users.plist with your first name, last name, gender and password. An [sic] plist is returned which contains the user's ID as well as other information such as the date of creation.
>
> **Figure 1**



2. https://api.path.com/3/moment/feed/home?all_friends=1

This API call uses basic HTTP authentication (with a certain key) to obtain some metadata about myself – from the binary plist file it looks like it contains my first name, last name, cover photo, profile picture, etc.

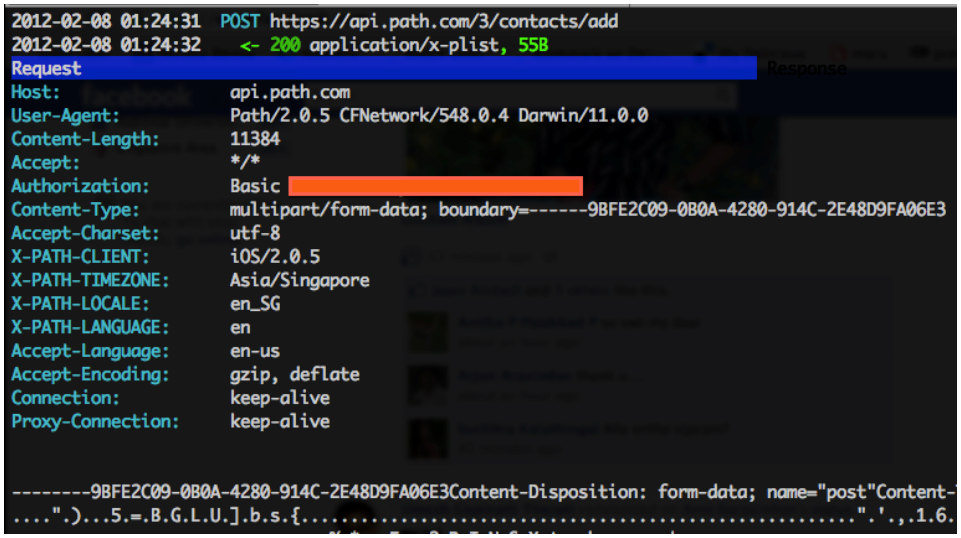
Figure 2



3. https://api.path.com/3/contacts/add

This is the actual offending call which uploads my entire address book to Path.

Figure 3



284. This is followed by normal API calls which among others, updates my location, fetches my activity stream and tracks events within the app using Mixpanel.[17]

285. Path's patent revealed its use of Plaintiffs' and Class Members' digital content affixed with GPS, contacts, and user metadata, to capture content derived from interactions:

> Patent application title: AUTOMATED AGING OF CONTACTS AND CLASSIFYING RELATIONSHIPS
>
> Inventors: David B. Morin (San Francisco, CA, US) Shawn D. Fanning (San Francisco, CA, US) Dustin R. Mierau (San Francisco, CA, US) Daniel S. Dofter (San Francisco, CA, US) Matthew M. Matteson (San Francisco, CA, US) Mark Lewandowski (San Francisco, CA, US) Mary Ann Brennan (San Francisco, CA, US) Daniel Trinh (San Francisco, CA, US) Mallory Paine (San Jose, CA, US)
> Assignees: Path, Inc.
> IPC8 Class: AG06F1516FI
> USPC Class: 709205
> Class name: Cooperative computer processing
> Publication date: 01/12/2012
> Patent application number: 20120011204
> Read more: http://www.faqs.org/patents/app/20120011204#ixzz1lzrcgzLU
>
> [0001] This application claims the benefit of priority to U.S. Provisional Application Ser. No. 61/363,081 filed Jul. 9, 2010, which application is incorporated by reference herein in its entirety. This application also claims the benefit of priority to

[17] Arun Thampi, *Path Uploads Your Entire iPhone Address Book To Its Servers*, Feb. 8, 2012, http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html (last accessed Aug. 8, 2013).

U.S. Provisional Application Ser. No. 61/494,388 filed Jun. 7, 2011, which application is incorporated by reference herein in its entirety

Claims:

1. A computer implemented method comprising: identifying one or more interactions between a first user and a second user within a social networking system; scoring each respective interaction of the one or more interactions based on a group score and a time penalty, wherein the group score is based on the number of users in the respective interaction and the time penalty is based on a time between a current time and a time of a last interaction between the first user and the second user; determining a relationship ranking that measures an affinity of the first user towards the second user, the relationship ranking comprising the one or more interaction scores; and sending to a client for display an indicator representing the relationship ranking between the first user and the second user. . . .

Detailed Description: . . .

Figure 4

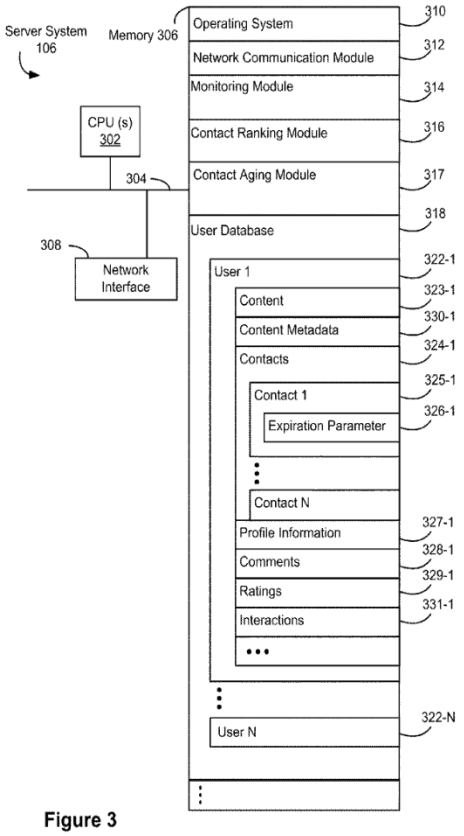


Figure 3

[0032] The user database 318 stores information for one or more users 322. In some embodiments, user database 318 is a distributed database. Information for a respective user 322-1 includes content 323, contacts 324, profile information 327, comments 328 and ratings 329, content metadata 330 and interactions 331. User profile information 327 stores information such as biographic, demographic and other types of descriptive information (work experience, educational history, hobbies or preferences, interests, location, and the like).

[0033] Comments 328 stored in the user database 218 include comments by the user as well as comments from other users on content associated with the user. Ratings 329 include the user's rating of content. Interactions 331 stores information about the user's interactions which includes a time of the interaction, the identifiers of other users involved in the interaction, the type of the interaction and weights associated with the interaction. The content 323 includes images, video, audio associated with the user. The content may be captured by the user or another user. The content metadata 330 includes descriptions or categories of content, tags of users and geographic location information. For example, the user may apply a category of "places" to a picture depicting a landmark.

"This is currently the industry's best practice": Mea Culpa?

286. Path CEO Morin's initial response to the public outrage over Path's activities was non-responsive. Rather than owning up to Path's misconduct and taking responsibility that Path violated its terms of use and users' trust, his response concerned an attempt to justify Path's activities:

> This is currently the industry best practice and the App Store guidelines do not specifically discuss contact information. However, as mentioned, we believe users need further transparency on how this works, so we've been proactively addressing this.[18]

287. Path's response was also without merit upon review of Apple's App Store guidelines: Path is an "Apple Developer" that agreed to the iOS Developer Agreement ("IDA") and the Program License Agreement ("PLA"). The IDA includes the following restrictions:

> 17.1: Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used
>
> 17.2: Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected[.]

288. The PLA provides additional obligations on third-party developers:

> 3.3.9. You and Your Applications may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising. You may not use analytics software in Your Application to collect and send device data to a third party.
>
> 3.3.10. You must provide clear and complete information to users regarding Your collection, use and disclosure of user or device data. Furthermore, You must take appropriate steps to protect such data from unauthorized use, disclosure or access by third parties. If a user ceases to consent or affirmatively revokes consent for Your collection, use or disclosure of his or her user or device data, You must promptly cease all such use.[19]

---

[18] Jon Mitchell, *The Price of Free: Path Uploads Entire Address Book To Its Servers*, Feb. 7, 2012, http://www.readwriteweb.com/archives/path_is_a_free_app_and_it_will_spy_on_us.php.

[19] Letter from Catherine A. Novelli, Vice President, Worldwide Gov't Affairs, Apple Inc., to Congressmen Waxman and Butterfield (Mar. 2, 2012), http://waxman.house.gov/sites/waxman.house.gov/files/Letter_CookResponse_03.02.12.pdf (last accessed Aug. 8, 2013).

289. Path's second attempt to diminish its public relations nightmare involved an attempt to provide a "Mea Culpa" of sorts, but then informed all users of its intent to continue to retain and store the unauthorized data in bulk. Path's CEO, Dave Morin, issued an "apology," reprinted in full, *supra*, at ¶ 110.

290. Path's third attempt to remedy complaints related to a rebuttal of an interview by its CEO in November 2010 in which he stated Path would not retain or store users' data:

> [Gawker: Is it correct that Path uses iPhone address book data? Thanks for any guidance!] . . .
>
> **Path does not retain or store any of your information in any way.**
>
> That help?
>
> Dave
>
> . . .
>
> [Update from Dave Morin]: Our email exchange from November 15, 2010 was absolutely accurate. That was the day Path launched and we were not storing any address book information at that time, as I clearly stated in my email. We introduced FriendRank in March 2011 and that is when we began retaining contact information with the intent to maximize the Path experience, specifically by:
>
> 1) showing users a list of friends on Path
> 2) suggesting friends users might want to connect to
> 3) telling users when any of their contacts joined Path
>
> Dave Morin, Co-Founder and CEO of Path.[20]

291. Path's claim that retaining contact information was necessary in order to "maximize" the Path user's experience reeked of Silicon Valley marketing rhetoric, in that stating it was actually necessary to keep user data after the user has found their friends on the Path App was false and misleading, since a hashing-enabled App could delete all the uploaded hashed data, and still allow the "friend-finding" process to work.

[20] Ryan Tate, *Don't Forgive Path, the Creepy iPhone Company that Misled Us Once Already*, Gawker (Feb. 8, 2012, 7:44 PM), http://gawker.com/5883549/dont-forgive-path-the-creepy-iphone-company-that-misled-us-once-already (emphasis added) (last accessed Aug. 8, 2013).

292. Path's claim that its interest was only to assist its users to locate friends within its App and that this benefited only its users and was not a "prodding" mechanism was also false and misleading:

> Consumer complaints: Path (company/product): When you add a photo on Path, does Path send email notifications to friends that you aren't sharing your Path with? I added a photo to Path recently, and at least one Facebook friend, who I wasn't sharing my Path with at the time, got an email saying "Richard sent you a photo using Path" (this language is somewhat misleading as I hadn't taken any action in relation to this person on Path, and they weren't relevant to the photo in any way).[21]

293. Path's storage of user data was vital to its immediate and continued growth, since it did not want to delay building its platform slowly while prospective users spent time locating the App, experimenting with its functions to determine if they would remain a user, and prompting its users to assist in referring users' contacts. Path's self-imposed limitation of users' friends, initially to fifty and then to 150, was a ploy to limit the upload and storage of unprofitable user content and to limit server costs. Path wanted the ability to create a database of users' data by monitoring of Interactions between users' contacts while in online social networks. If Path was successful, it would allow it to eventually drop its connection to these underlying social networks. In the meantime, Path would avoid the limitations involved with the mobile App ecosystem and monetize the existing platform of online social networks.

294. Path's business plan concentrated on exponential growth, relying on the data derived from the Interactions between users and their contacts, and not exclusively from user-only data. By calculating and pruning its users' Interactions with their contacts on multiple online platforms, it allowed Path to preserve its own platforms and servers. This core infrastructure of Path's mobile platform derived from the Facebook Platform Connect concepts, both co-invented by Path CEO David Morin.

---

[21] Quora, *Path (company/product)*, http://www.quora.com/Path-company-product/When-you-add-a-photo-on-Path-does-Path-send-email-notifications-to-friends-that-you-arent-sharing-your-Path-with (last accessed Aug. 8, 2013).

295. The limitation of users initially to fifty and then to 150 may have been marketed to promote the App as being meant for close connections, but in actuality it allowed Path to limit the cost to develop its own platform and to use existing platforms, such as Facebook, which had almost one billion users. Following principles similar to those known as "Metcalfe's Law"—a principle that states that a network's value is proportional to the square of the number of connected users of the system—Path's intent was exponential growth using its users' contacts. Path reports it now has in excess of two million users. Such a database of actual users could then potentially produce a source of a few hundred prospective contacts for each user, then leading to a user base of hundreds of millions of users, rivaling the largest social networks. By amassing data derived from users' contacts, and not just users, Path's unauthorized data collection practices allowed immediate growth.

296. Path's fourth attempt to repel criticism related to deleting all data obtained that resided on Path's servers: "We've deleted the entire collection of user contact information from our servers. . . . Unlike some other companies, we believe that users should have complete control over their data. This is just the right thing to do."[22]

297. While Path's attempts to justify its activities failed, its responses were also without merit. Path's provisional application, "System and Method for Social Interaction with Geolocation and Automated Aging and Pruning of Interactions and Contacts," revealed its actual intent related to user contact address data collection, retention and storage four months before the *Gawker* interview and subsequent rebuttal. Path CEO Morin's attempts to justify Path's activities, attempting to parse the meaning of "privacy," was more of a set of rejoinders of varying degrees of flippancy and superciliousness:

- "We don't want to connect you with just anyone on Path."
- "We used the data for the sake of simplicity."

[22] Jon Mitchell, *Path CEO: "We Thought We Were Doing This Right,"* Wired (Feb. 8, 2012, 4:40 PM), http://www.wired.com/gadgetlab/2012/02/path-dave-morin-explains-data/ (last accessed Aug. 8, 2013).

- "The problem is that the word privacy means so many things. We all have different ideas, there is no real standard."

Hipster

298. Hipster has already been served with process twice in the above-captioned lead case through its registered Delaware agent for service of process, Agents and Corporations, Inc., 1201 Orange Street, Suite 600, One Commerce Center, Delaware 19801, but has not appeared and default has been entered against it on the Plaintiffs' Second Amended Complaint. ECF Nos. 103, 346. Solely as against Hipster and in furtherance of that entry of default and to pursue default judgment, Plaintiffs (Plaintiff King particularly) from the lead *Opperman* case maintain the allegations and claims of their Second Amended Complaint, ECF No. 103, against Hipster. Accordingly, the current pleading is not meant to amend the prior complaint as to Hipster.

Foursquare

299. App Defendant Foursquare Labs built the *Foursquare* App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the *Foursquare* App on the App Store and served as Foursquare Labs's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

300. Plaintiffs Beuershasen, Hoffman, King, Mandaywala, Paul, Sandiford and Varner (the "Foursquare Plaintiffs") obtained the Foursquare App and recall signing up and logging in on the Foursquare App's sign-up/log-in screen prior to February 2012 and then using and navigating around the App.

301. The Foursquare Plaintiffs do not recall being presented either then, before downloading or before launch of the Foursquare App with an alert or warning indicating that the Foursquare App would upload or transmit Plaintiffs' private mobile address book to Foursquare Labs or anyone else.

302. Published reports state that before February 2012 when users like these Plaintiffs signed up without warning the Foursquare App automatically uploaded all email addresses and phone numbers in the iDevice owner's private mobile address book in-bulk via Wi-Fi, 3G and the Internet to unintended recipient Foursquare Labs.

303. As determined in a posted analysis by *Tapbot* App founder Paul Haddad,

> "Foursquare [ ] was uploading all of the email addresses and phone numbers in [a user's] address book with no warning and no explicit consent given ."
>
> "Foursquare also seems to be sending out phone numbers for contacts as well. This is on launch, after creating a new account."
>
> "Foursquare 4.2 (latest), Sends out all email address in address book via HTTPS, no warning, no hashing."

304. Foursquare Labs' communications director verified in press e-mails that the App "transmit[ted] the address book information," thus confirming Mr. Haddad's analysis.

305. Prior to February 6, 2012, the Foursquare App's "Connect with your friends" screen would instantly display how many of the user's "contacts are on foursquare" because it had already uploaded and Foursquare Labs had analyzed the user's address book before the used reached that screen.

306. Accordingly, Foursquare Labs has wrongfully obtained, retained, disclosed and de-privatized the Foursquare Plaintiffs' valuable private address books and used their iDevices without seeking (or obtaining) authorization to do so. Foursquare Labs and its App never asked the Foursquare Plaintiffs if they could do any of these things.

307. On information and belief, the Foursquare Plaintiffs' mobile address books were not hashed to protect its anonymity before being transmitted to Foursquare Labs' servers.

308. Around late February, 2012, Foursquare Labs modified its App to include the following programmatic halt and pop-up alert:

> "**Searching for friends who are using foursquare?** To find your friends, we send your address book information to our servers. Don't worry, it's sent securely and we don't store it! [Noooo!] [Ok]"

Instagram

309. App Defendant *Instagram* (including its above-identified predecessors-in-interest) built the *Instagram* App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted, and deployed the *Instagram* App on the App Store and served as *Instagram*'s world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

310. The *Instagram* App launched in October 2010. The *Instagram* App was made available through the Apple App Store for iDevice users.

311. The *Instagram* App was promoted as an image sharing service, which facilitated shooting, processing, and sharing of images across services, including social services like Facebook, Twitter, Foursquare, or *Instagram*'s own website.

312. The App permitted modification of images though the addition of frames and filters, to, for example, transform the image to make it look like it was taken with an old-style Polaroid camera.

313. On *Instagram*'s iTunes user page, no End-User License Agreement ("EULA") or privacy policy was presented to potential users.

314. A user initiated the *Instagram* App on their iDevice by navigating to the *Instagram* website, and clicking a "sign up" button on their screen. The sign up screen required a user to open an account with *Instagram*. The user was required to input their first and last name, their email address, and pick a username. During the sign up process, no EULA or privacy policy was presented to users.

315. Immediately upon establishing the account, the *Instagram* App, automatically and without notification or consent, uploaded the contents of the user's contact address book to *Instagram* servers, including first and last names, telephone numbers, and email addresses.

316. Plaintiffs Arabian, Biondi, Dennis-Cooley, Green, Hoffman, King, Mandaywala, Moses, Sandiford, and Varner (the "*Instagram* Plaintiffs") recall using and navigating around the *Instagram* App.

317. One or more of the *Instagram* Plaintiffs recalls signing in, navigating within the *Instagram* App to a "Find friends" screen, tapping a displayed "From my contact list" button bar, and then being presented with a list of recognizable names that the Plaintiff could choose to "follow" by pressing another button near each name.

318. The *Instagram* Plaintiffs do not recall being presented at the time with any intervening alert or pop-up dialogue box warning them that their mobile address book had to or would be transmitted to *Instagram* to perform this function.

319. Published reports (which show mitmproxy test screenshots) showed that when *Instagram* App users tapped the "From my contact list" button bar, the owner's iDevice initiated an unauthorized call and transmitted in-bulk, unencrypted, and in plain text to *Instagram*'s servers all of the first names, last names, email addresses and phone numbers from the user's iDevice mobile address book.

320. *Instagram* thus obtained, retained, disclosed, and de-privatized the identified Plaintiffs' valuable private mobile address books and used their iDevices without seeking (or obtaining) permission to do so. Prior to February 2012, neither *Instagram*, nor the *Instagram* App ever asked Plaintiffs if they could do this. Plaintiffs were not asked to consent to the taking or transmission of their address books. Plaintiffs never consented to bulk lists of email addresses, phone numbers, contact names, or other fields of data in their iDevices's mobile address book being uploaded and transferred to *Instagram*'s servers or to that data being used, manipulated or stored elsewhere than on his or her iDevice.

321. On information and belief, *Instagram*, via the *Instagram* App and with Apple's assistance, caused Plaintiff's iDevice to initiate this unauthorized transmission and upload for *Instagram*'s discretionary remote use and storage extensive bulk portions of Plaintiffs' valuable private mobile address books, all without seeking Plaintiffs' consent.

322. On information and belief, the Plaintiffs' mobile address book was not cryptographically hashed before being relayed and transmitted to *Instagram*'s servers.

323. In mid-February 2012, a revised version of the *Instagram* App was quietly issued that included a programmatic halt and the following new pop-up alert that appeared when a user tapped the "From my contacts list" button bar on the "Find Friends" page:

> "**Search for Your Friends in Address Book?** In order to find your friends, we need to send address book information to *Instagram*'s servers using a secure connection. [Cancel] [Allow]."

Instagram, though, could easily have elected to use anonymized hashed data to blind match users "friends" without ever needing any of the raw address book materials.

324. Beginning in October 2010, and continuing from the date of the introduction of the App up until at least February 2012, *Instagram* did not inform any users that the contact address book would be copied, uploaded, or retained.

325. Between October 2010 and December 2010, it was reported that *Instagram* enticed over one million iDevice users to download the *Instagram* App. In each case, from the time the *Instagram* App was made available until approximately February 2012, the *Instagram* App, without notice or consent to any user, immediately upon signing up, uploaded the contents of the user's contact address book to its servers, and retained that information. In this manner, *Instagram* thus obtained the first and last names, phone numbers, and email addresses contained in the iDevices of over one million users. If the average number of contact address book entries per user was even a low as twenty entries per iDevice (some users report over 10,000 contacts – there appears to be no maximum number of contacts that an iDevice can store), *Instagram*, in a period of less than three months, obtained more than 20 million names, phone numbers, and email addresses without anyone outside the company realizing or understanding what *Instagram* had acquired.

326. In June 2011, *Instagram* announced it had 5 million users. In September, 2011, *Instagram* surpassed 10 million users.

327. When *Instagram* introduced its App on the Internet, it did so with the following language:

Meet Instagram.

It's a **fast**, **beautiful** and **fun** way to share your life with friends through a series of pictures.

Snap a photo with your iPhone, choose a filter to transform the look and feel, send to Facebook, Twitter or Flickr – it's all as easy as pie. It's photo sharing, reinvented.

Oh yeah, did we mention it's free?

328. Overlaying an image of an iPhone running the Instagram App was a large star-like overlay in bold capital letters: "FREE DOWNLOAD."

329. In fact, the Instagram App was not "FREE." Contrary to Instagram's representations, users paid a significant, though completely undisclosed, price for the App.

330. Essentially, and literally, *Instagram* "stole" the contact address book, not only of the Plaintiffs, but of millions of additional users.

331. The App that *Instagram* users downloaded was represented to them to be "a fast, beautiful and fun way to share your life with friends through a series of pictures." Instead, the App was a Trojan horse—one that allowed *Instagram* to collect millions of contact names, phone numbers, and email addresses from its unsuspecting users, without ever having to go out in the marketplace to buy those contacts, if such a list could even be had at any price.

332. By stealing contact information, *Instagram* was able to achieve a remarkable and unprecedented benchmark within the hot and developing social networking community. Within a year and a half of its launch, *Instagram* had become a company that was valued at $1 billion, and

that valuation was made concrete when Facebook paid $1 billion in cash and stock to purchase the company. On information and belief, and Plaintiffs thereupon allege, the value of the contacts and connections *Instagram* acquired by stealing the contact address books of millions of its customers was instrumental in achieving that $1 billion valuation.

333. When *Instagram* took a user's contact address book, the user was not notified that the contact address book was part of the bargain. All users were presented with was vague information about the benefits and attributes of the *Instagram* App. In none of those descriptions were users informed that the contact address book was the quid pro quo for the downloaded App. Other iDevice Apps were forced to offer more value when they disclosed that the contact address book was part of the price for use of the App. In this way, *Instagram* cheated the user (and other Apps that told the truth) by not disclosing the true cost of the use of the *Instagram* App.

334. Had users known the true cost of the *Instagram* App, they would not have agreed to download it. Users' investment in time, energy, and creativity to build and maintain their contact address book was worth far more money than the *Instagram* App ostensibly traded for. Thus, users were deprived of the true measure of benefits that their contact address book information could have been exchanged for.

335. *Instagram*'s conduct in overriding Apple's purported protections of users' privacy and security devalued the iDevice for its users. Users would not have purchased an iDevice or, alternatively, would not have paid as much for it had they known that the *Instagram* App would circumvent both internal and external safeguards designed for the protection of their private and personal information residing on the iDevice.

336. Because users were tricked into downloading the *Instagram* App, believing that the price and consequences of the downloaded App were different than *Instagram* represented they were, any use of the *Instagram* App was achieved by and through fraud and deception. All use of the *Instagram* App after being downloaded by users was based upon the intentional dissembling by *Instagram* of the App's true cost.

337. Based upon this deception by *Instagram*, iDevice users lost storage space on their iDevice—storage space which could have been utilized instead for a legitimate App that had disclosed its true costs of use. Thus, the false pretenses under which the *Instagram* App was downloaded caused actual harm: the diminution of the actual value of an iDevice that had the *Instagram* App installed upon it which overrode privacy and security settings and protections built into the ordinary use of the iDevice. Had users known of *Instagram*'s ability to override and ignore these privacy and security protections, they would not have purchased the iDevice or they would not have paid as much for it.

338. Based upon this deception by *Instagram*, iDevice users incurred impaired battery life, in that each use of the *Instagram* App (both its known and unknown features) utilized the battery each time it was active on the iDevice. The iDevice battery is not an infinite resource. The battery must be regularly recharged. It may not, however, be infinitely recharged. The charge and discharge cycle of the battery causes chemical changes in the active battery material, diminishing the battery's storage capacity and requiring even more frequent recharging. Thus, each activation of the *Instagram* App and its access and utilization of the finite iDevice battery power, for both disclosed and undisclosed functions, contributed directly to the ultimate demise of the battery. iDevice users could have instead utilized their finite battery life for a legitimate App that had disclosed the true costs of its use. Thus, the false pretenses under which the *Instagram* App was downloaded, installed, and run on the user's iDevice caused actual harm in the diminishment of the life of the battery for the iDevice.

339. Based upon this deception by *Instagram*, iDevice users face the necessity of expert removal of the *Instagram* App from their iDevices. The costs to hire a technician who can knowledgeably, effectively, completely, and permanently remove the *Instagram* App, and all its code, both disclosed and undisclosed, is substantial. The knowledge required from such an operation is not easily obtained outside of Apple itself. Thus, the false pretenses under which the *Instagram* App was downloaded, installed, and run on the user's iDevice caused actual harm to users in necessitating expensive expert removal of the *Instagram* App and all of its code, both

disclosed and undisclosed, from the iDevice in order to restore the device to its previously secure state.

340. Contact address books are stored in the memory of the user's iDevice. The user has the option to create a duplicate copy on a personal, stand-alone system (syncing) which they control, but in all cases, the contact address book is not otherwise shared, transmitted, broadcast, or otherwise divulged on publicly accessible channels. Unless the user physically relinquishes custody of his or her iDevice to another individual, without express permission, no one other than the iDevice's owner ever has access to the contact address book.

341. *Instagram* violated this exclusive control when it took, without notice, the contact address book and uploaded it to its servers. The *Instagram* App did not bother with any type of encryption. The copying and transmission of the contact address book from the iDevice to the *Instagram* servers was effected "in the clear." When *Instagram* transmitted a copy of the user's contact address book "in the clear"—which means it was done without any encryption whatsoever—the user's contact address book was publicly disclosed. Any and all strangers who monitor web transmissions had complete and unrestricted access to unencrypted transmissions that utilized "in the clear" transmissions.

342. The design of the iDevice, and specifically the iDevice design that stores, accesses, and utilizes the contact address book exclusively within the physical boundaries of the iDevice unit itself is a central component of the iDevice function. This functionality insures that the contact address book remains within and under the complete control of the iDevice owner. This functionality insures that the contact address book retains its confidentiality.

343. When *Instagram* copied, uploaded, and stored the contact address book to its servers in the cloud, *Instagram* broke these aspects of the iDevice's functionality. Once *Instagram* copied, uploaded, and stored the contact address book on its servers in the cloud, the functionality of the iDevice's design that deals with its contact address book was broken in at least two respects: (1) the iDevice was designed to keep the contact address book under the complete control of the device's owner; and (2) the iDevice was designed such that the contact address book would stay safely,

securely, and confidentially within the confines of the iDevice hardware. Both of these design aspects of the iDevice were destroyed by *Instagram*'s App.

344. Individuals that downloaded the *Instagram* App must now request that *Instagram* remove their data from its servers. Individuals that never downloaded *Instagram*'s App but are named within Plaintiffs' and Class Members' contact address book data will have no notice of *Instagram*'s action so as to request *Instagram* to delete their personal information.

345. *Instagram*'s actions were surreptitious and so were conducted without authorization and exceeding authorization.

346. Plaintiffs were not made aware of, nor did they consent to the taking of this data, and there was no way to opt out of this surreptitious collection of information. The information collected included, but was not limited to, a Plaintiff's contacts and the interactions with their contacts.

347. As a result, Plaintiffs had the resources of their iDevices consumed and diminished without permission. Such resources were measurable and of actual value, and included iDevice storage, battery life, and bandwidth from Plaintiffs' wireless services provider. The monetary value of the resources taken from Plaintiffs are quantifiable. The rate at which battery charge was diminished on the iDevices as a result of *Instagram*'s actions was material to Plaintiffs, particularly given the power resource constraints on the iDevices—*Instagram*'s repeated actions during App executions utilized a portion of battery capacity with each action due to the power requirements of CPU processing, file input and output actions, and Internet connectivity.

Yelp!

348. App Defendant Yelp built the Yelp! App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Yelp! App on the App Store and served as Yelp's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

349. Plaintiffs Biondi, Hodgins, Hoffman, Mandaywala, Paul, and Sandiford, each recall navigating to various screens on and using the Yelp! App. They recall providing a log in and navigating within the Yelp! App to a screen containing a ["Find Friends"] button with the accompanying displayed text:

> "Find friends on Yelp using your Contacts and Facebook friends? You'll be able to see their bookmarks and find out when they're nearby. [Yes, Find Friends] [No, Skip This]",

and pressing the ["Yes, Find Friends"] button. Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the *Yelp!* App would transfer any portion of his or her private mobile address book to Yelp to perform this function or warning that such a transmission was about to occur.

350. The displayed Yelp! App text does not request permission to upload any address book materials from Plaintiffs' iDevices or externally transmit any of Plaintiffs' mobile address book material.

351. Published reports indicate that before February 2012 when an iDevice Yelp! App user tapped the ["Yes, Find Friends"] button, the iDevice would automatically, without first asking for or securing consent to do so, initiate a call, copy bulk portions of the user's address book, and the iDevice would then relay, upload and transmit those materials via Wi-Fi, 3G and the Internet to Yelp's servers, where Yelp then at its discretion remotely stored, used and kept the materials. This occurred to the identified Plaintiffs multiple times.

352. Yelp thus obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without seeking (or obtaining) authorization to do so. Yelp and its App never asked Plaintiffs if they could do any of these things.

353. Following adverse media reports, Yelp modified its App in mid-February 2012 with a new halt and an alert that appeared when a user tapped the ["Find Friends"] button that reads:

> "**Find Friends** To find friends, we'll need to upload your contacts to Yelp. Don't worry, we're not storing them. [No Thanks] [OK]"

Twitter

354. App Defendant Twitter built the Twitter App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Twitter App on the App Store and served as Twitter's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

355. Plaintiffs Beuershasen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul and Varner (the "Twitter Plaintiffs") recall opening the Twitter App, signing up via its displayed registration screen, and using the App. They were initially presented a "Welcome" screen prompting them to press an on-screen button labeled ["Follow your friends"], under which was written in small type: "Scan your contacts for people you already know on Twitter." They also recall another screen labeled "Follow Friends" that similarly prompted them to press an on-screen button labeled ["Follow your friends"], under which was written in small type the identical phrase as before.

356. The App's ["Follow your friends"] button-bar and accompanying textual phrase do not request for permission to upload or transmit elsewhere any of the Plaintiffs' iDevice address book materials.

357. As prompted, prior to February 2012, each Plaintiff pressed the displayed ["Follow your friends"] button-bar. Plaintiffs recall no alerts or warnings that their private mobile address books were being taken.

358. According to Twitter, when Twitter App users tapped the ["Follow your friends"] button-bar prior to February 2012, the App connected their iDevice to Twitter's servers uploaded all email addresses and phone numbers in the iDevice owner's mobile address book, which Twitter used, stored and kept for eighteen months or so (likely in unsecure plain text). This occurred to the identified Plaintiffs.

359. After media questioned the Twitter App's privacy practices and secret address book collection function, sometime after February 6, 2012 Twitter modified the language on its Twitter

App's "Find Friends" screen and ["Follow your friends"] button, replacing the phrase "scan your contacts" with the phrase "upload your contacts" (thus essentially conceding the non-equivalence of those words) and also added the following intervening alert:

> "**Find Friends on Twitter** We will securely upload your contacts to help you find friends and suggest users to follow on Twitter. [Cancel] [OK]"

Foodspotting

360. App Defendant Foodspotting built the Foodspotting App using Apple-supplied components and tools, with Apple providing substantial assistance through the Program and a digital certificate for the App to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Foodspotting App on the App Store and served as Foodspotting's world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users.

361. Plaintiffs King and Sandiford (the "Foodspotting Plaintiffs") recall opening the Foodspotting App, signing up via its registration screen, and using the App. More particularly, they recall navigating to the Foodspotting App's "Follow People" screen containing an on-screen button labeled ["Find iPhone Contacts."]. While on that screen, the Foodspotting Plaintiffs tapped that button. The screen contained no warnings whatsoever indicating that the App was relaying his or her mobile address book to Foodspotting.

362. The displayed button and screen menu name do not constitute a request for permission or transmit or upload Plaintiffs' iDevices address book materials and Plaintiffs did not consent to this.

363. According to defendant Foodspotting's February 15, 2012 company blog, when App users tapped the ["Find iPhone Contacts]" button, the iDevice would, silently and without first asking or securing consent, initiate an Internet call, copy bulk portions of the user's address book (in particular, all email addresses), and the iDevice would then relay and transmit those materials via Wi-Fi, 3G and the Internet to Foodspotting's servers, where Foodspotting then remotely used and stored the materials. Upon information and belief, this occurred to the Foodspotting Plaintiffs

multiple times. Reports indicate the transmission was insecure and included the user's "unencrypted address book data [… with] a list of email addresses in plain text."

364. Foodspotting has obtained, retained, transmitted, disclosed and de-privatized these Plaintiffs' valuable private mobile address books and used their iDevices without seeking (or obtaining) authorization to do so. Foodspotting and its App never asked Plaintiffs if they could do any of these things.

365. Following adverse media reports, Foodspotting announced it had "address[ed] address book concerns" in its modified App by adding "extra permissions and security," including a new pop-up alert/dialogue box to its App's "Follow People" page and ["From iPhone Contacts"] button. Foodspotting reportedly updated its App at that time to also employ HTTPS transmissions.

Angry Birds Classic/Crystal - Rovio & Chillingo

366. Defendant Rovio built the Angry Birds Classic App using Apple-supplied components and tools.

367. Integrated into the Angry Birds Classic App is Chillingo's Crystal platform (which, on information and belief, is an App itself). On information and belief, Chillingo's Crystal platform is integrated into many gaming Apps offered on the App Store, either by Defendant Chillingo or the game developer.

368. On information and belief, Chillingo built Crystal using Apple-supplied components and tools.

369. On information and belief, either (a) Chillingo licensed the Angry Birds Classic App from Rovio, integrated the Crystal platform into it, then released it for the App Store, (b) Rovio integrated the Crystal platform into its own App, which it self-released for the App Store, or (c) Chillingo and Rovio work together to release an App containing both the Angry Birds Classic and Crystal features. Nevertheless, to consumers it appears as an integrated product.

370. Apple provides substantial assistance through the Program and a digital certificate for the Angry Birds Classic App (and possibly an additional certificate the Crystal platform) to function on iDevices. Following Apple's review (during which time Apple learned or should have

learned of the App's malicious, prohibited features), Apple released, promoted and deployed the Angry Birds Classic App on the App Store and served as the world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users. The Angry Birds Classic App was and is available in both free and paid versions on the App Store.

371. Plaintiffs Beuershasen, Dean, Green, Hodgins, Mandaywala, Sandiford and Varner (the "Angry Birds Plaintiffs") recall opening the Angry Birds Classic App, playing some games of Angry Birds, and navigating around to other screens and menus within the App. One or more Plaintiffs recall after signing up on the integrated Crystal platform navigating within the Angry Birds Classic App to a "Send an invite" screen (with the subheading "Invite your friends to Angry Birds"), and pressing the button bar labeled "Invite from contacts" with the subheading "Send an invite from your local Contacts." The Angry Birds Plaintiffs do not recall being presented at any time in that process with an intervening alert or pop-up display indicating that the App (or Apps) would upload or transmit elsewhere any part of his or her private mobile address book or warning that such a transmission was about to occur.

372. Either Chillingo, Rovio or both companies wrote, selected and approved the in-App language on this screen and button bar.

373. The displayed in-App text did not ask to transmit or upload any address book materials from Plaintiffs' iDevices in bulk or otherwise.

374. Published reports containing mitmproxy data-flow screen shots indicate that before February 2012 when an iDevice Angry Birds Classic App user tapped the ["Invite from contacts"] button, the iDevice would automatically and without asking connect via the internet and transmit bulk portions of the user's private mobile address book to one or both companies' servers, which stored and remotely used the materials.

375. Reportedly, the uploaded user address book materials may also have been transferred to other third-parties and Google.

376. Rovio and/or Chillingo have thus obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without seeking (or

obtaining) authorization to do so. Rovio and Chillingo (and their Apps) never asked Plaintiffs if they could do any of these things.

377. Rovio and Chillingo were both aware of the features and operations of the other's product, were cognizant of the relaying of iDevice owners' mobile address books, and collaboratively participated in, assisted and enabled those activities to occur.

378. Rovio nevertheless publicly represented that "No contact information is collected or stored by Crystal." On information and belief, that statement is not true.

379. Before February 2012, Rovio never notified the identified Plaintiffs that the integrated Angry Birds Classic App would cause their iDevices to make an unauthorized Internet call, upload in bulk or transmit any part of their private mobile address book materials to remote locations. Nor did Chillingo.

380. Before February 2012, Rovio never notified the identified Plaintiffs that Rovio or any other third party would be manipulating or using their mobile address book materials at a remote location. Nor did Chillingo.

381. On information and belief, in mid-February 2012 (i.e., after reports and privacy concerns surfaced about Apps violating their users' privacy), either Rovio or Chillingo added a new alert box to the integrated Angry Birds Classic App's "Send an invite" screen that included language stating that pressing that button would cause the "upload" of the user's mobile address book materials to Rovio's or another party's computer server.

382. Chillingo and Rovio are jointly and severally liable on the claims alleged herein pertaining to the Angry Birds Classic App.

Cut the Rope/Crystal - ZeptoLab, Chillingo & Electronic Arts

383. On information and belief, App Defendant ZeptoLab built the *Cut the Rope* App.

384. Apple's iTunes *Cut the Rope* page identified Chillingo as the "publisher" of the *Cut the Rope* App.

385. Chillingo's Crystal platform is integrated into the *Cut the Rope* iDevice App.

386. On information and belief, either (a) Chillingo licensed the *Cut the Rope* App from ZeptoLab, integrated the Crystal platform into it, then released it for the App Store, (b) ZeptoLab integrated the Crystal platform into its own App, which it self-released for the App Store, or (c) Chillingo and ZeptoLab worked together to release an App containing both the *Cut the Rope* and Crystal features. Nevertheless, to consumers it appears as an integrated product.

387. Apple provides substantial assistance through the Program and a digital certificate for the *Cut the Rope* App (and may provide an additional certificate for the Crystal platform) to function on iDevices. Following Apple's review (during which time Apple learned or should have learned of the App's malicious, prohibited features), Apple released, promoted and deployed the *Cut the Rope* App on the App Store and served as the world-wide agent for the solicitation of orders for and the delivery of the App to iDevice end-users. The *Cut the Rope* App was and is available in both free and paid versions on the App Store.

388. Plaintiffs Biondi, Green, Hodgins, Mandaywala, Sandiford and Varner (the "*Cut the Rope* Plaintiffs") recall opening the *Cut the Rope* App, playing some games of *Cut the Rope*, and navigating around to other screens and menus within the App. More particularly, one or more Plaintiffs recall after signing up on the integrated Crystal platform navigating within the *Cut the Rope* App to the "Find friends" screen and pressing the button bar labeled ["Find friends via contacts"].

389. Either Chillingo, ZeptoLab or both companies wrote, selected and approved this in-App text.

390. The *Cut the Rope* Plaintiffs do not recall any intervening alert or pop-up or warning indicating that depressing that button would transmit elsewhere or upload any part of his or her private mobile address book.

391. The displayed in-App text does not ask to upload, transmit or transfer elsewhere any address book materials from Plaintiffs' iDevices.

392. Published reports indicate that before February 2012 when an iDevice *Cut the Rope* App user tapped the ["Find friends via contacts"] button, the iDevice would automatically without

asking connect via the Internet and transmit bulk portions of the user's private mobile address book to one or both companies' servers, which stored and remotely used the materials.

393. The App (or Apps) thus took control of these Plaintiffs' iDevices and without instruction from the Plaintiffs to do so, ran an I/O function that called up the iDevice's mobile address book, contemporaneously intercepted the responsive I/O communication containing mobile address book information, initiated an Internet transmission that Plaintiffs never instructed their iDevices to make, and uploaded and publicly broadcast the intercepted mobile address book communication over the Internet, whereby ZeptoLab or Chillingo obtained the identified Plaintiffs' mobile address books (or substantial portions thereof). The transmissions were delivered over Wi-Fi, 3G and the Internet to ZeptoLab or Chillingo's servers. In the transmission process those private materials were publicly exposed to others via Wi-Fi and the Internet. This happened to Plaintiffs, on information and belief, multiple times.

394. On information and belief, the non-consensually uploaded user address book materials were transferred to ZeptoLabs' and/or Chillingo's computer servers, to other third parties and, reportedly, to Google.

395. As a consequence, ZeptoLab and/or Chillingo obtained and was able to retain, keep, remotely store, and use at its discretion the identified Plaintiffs' private mobile address book materials.

396. ZeptoLab and/or Chillingo thus obtained, retained, disclosed and de-privatized these Plaintiffs' valuable private address books and used their iDevices without seeking (or obtaining) authorization to do so. ZeptoLab and Chillingo (and their Apps) App never asked Plaintiffs if they could do any of these things.

397. Plaintiffs do not recall being presented with any alert or notification stating that any portion of their private mobile address book materials would be sent or disclosed to ZeptoLab, Chillingo or any other third party.

398. Plaintiffs were never informed that (and thus never consented to) any portion of their iDevice mobile address book materials being uploaded or transferred to ZeptoLab's or Chillingo's

servers or that Chillingo or ZeptoLab would obtain, possess, store and remotely use any of their private mobile address book materials.

399. On information and belief, ZeptoLab and Chillingo were both aware of the features of the other's product, were cognizant of the relaying of iDevice owners' mobile address books, and participated in, assisted and enabled those activities to occur.

400. On information and belief, ZeptoLab and Chillingo engaged in these actions with the assistance, support, encouragement and/or direct participation of each other and/or Electronic Arts.

401. On information and belief, sometime around February 17, 2012 (after reports privacy concerns surfaced about Path's unauthorized acquisition of its users' private mobile address books), ZeptoLab (or Chillingo) added a new alert box to the *Cut the Rope* App stating that activation of the "find friends" feature would result in the "upload" of the user's mobile address book materials to ZeptoLab's or another party's computer server.

402. ZeptoLab and Chillingo are jointly and severally liable on the claims alleged herein pertaining to the *Cut the Rope* App.

Chillingo

403. Chillingo operates a program oriented toward gaming apps and their developers (the "Gaming Program"). To participate in the Gaming Program, app developers must register with Chillingo, who operates and manages the Program.

404. Chillingo's Gaming Program helps registrants build apps and also enables registrants to integrate or incorporate Chillingo's Crystal into their apps.

405. Rovio and Zepto were both registrants in the Gaming Program.

406. In use, Chillingo's Crystal creates a networked leaderboard structure operated by Chillingo for those registrant apps and their users.

407. The Gaming Program affects and is involved in interstate commerce. For instance, businesses and individuals from all fifty states and internationally regularly communicate through and with the Gaming Program via the Internet. Chillingo, via the Program, regularly integrates Crystal via the Internet into Apps from around the world.

408. Rovio and ZeptoLab have communicated with or through the Gaming Program, associated with Chillingo through the Gaming Program, and had Crystal integrated into their Apps through the Gaming Program.

409. Chillingo, Rovio and ZeptoLab were each aware that their apps were designed to, and were, uploading portions of iDevice owners' mobile address books to Chillingo's or Rovio's or ZeptoLab's servers. Each was also aware that explicit permission had not been requested to do so.

Electronic Arts

410. Defendant Electronic Arts acquired Chillingo around October 2010 and has operated Chillingo as a reporting division or wholly-owned, joint-reporting subsidiary of Electronic Arts.

411. On information and belief, Electronic Arts has controlled Chillingo since October 2010 and directed and is aware of its business operations, including with respect to Crystal and the Gaming Program.

412. On information and belief, Electronic Arts is a successor-in-interest to or is vicariously liable for Chillingo's obligations and liabilities, including its joint and several liabilities alleged herein pertaining to the *Cut the Rope* App, the Angry Birds Classic App, and the Crystal platform.

Facebook

413. Facebook presently operates under a 20 year FTC Consent Decree for previously committing consumer privacy violations.

414. In late 2011, Facebook conducted due diligence on *Gowalla* for a contemplated business transaction with *Gowalla* and/or *Gowalla*'s owners. The contemplated transaction involved transfer of all or substantially all of *Gowalla*'s assets, technology, know-how or equity to Facebook.

415. During due diligence, Facebook learned that the *Gowalla* App incorporated the above-discussed contained computer contaminants that had adversely impacted users' privacy and that *Gowalla* had surreptitious harvested its users' private mobile address book without seeking

consent, resulting in substantial potential liabilities and creditor obligations for *Gowalla* to users of the *Gowalla* App (like these Plaintiffs and the Class members).

416. As a result, *Gowalla*'s management and owners and Facebook structured and executed a transaction with *Gowalla* around late 2011 to early 2012 designed to fraudulently transfer desired *Gowalla* personnel and substantially all existing *Gowalla* company assets (including technology and know-how relating to the *Gowalla* App) to Facebook in violation of California's Uniform Fraudulent Transfer Act, Cal. Civ. Code § 3439 The fraudulent transaction crafted by Facebook, *Gowalla*, and *Gowalla*'s management and owners redirected to *Gowalla*'s management and owners consideration properly due to *Gowalla* for its assets, which could (and should) have been used to satisfy creditor claims, including Plaintiffs' claims in this case.

417. Facebook did not pay *Gowalla* reasonably fair value for the *Gowalla* assets, technology, know-how or personnel. Facebook instead paid *Gowalla*'s shareholders and management for the company's assets. On information and belief, Facebook made payments of cash and/or Facebook pre-IPO stock to *Gowalla*'s stockholders and management (instead of *Gowalla*) in consideration for this transaction.

418. In connection with the transaction, Facebook merged and incorporated *Gowalla* assets and personnel into Facebook's ongoing business. As a result, Facebook acquired *Gowalla* rights to assets and key employees sometime after December 2011, leaving *Gowalla* effectively headless, lacking independent (or any) continuing management, and insolvent.

419. Accordingly, Facebook is a successor-in-interest to *Gowalla* (and to its liabilities, obligations and creditor claims, including Plaintiffs' claims asserted herein against *Gowalla*).

420. Facebook is also directly liable for *Gowalla*'s actions, liabilities and obligations (including those related to the *Gowalla* App) for actions from late-2011 through at least March 2012 (and possibly extending to the present).

421. Beginning in late 2011, Facebook operated, supervised and controlled *Gowalla* as a captive entity and the companies failed to properly maintain corporate formalities and separateness from one another.

422. For instance, *Gowalla* CEO Josh Williams and other *Gowalla* management and executive personnel contemporaneously worked for both *Gowalla* and Facebook, who paid substantially all of their salaries. *Gowalla* further reported in corporate filings that it lacked board or any executives.

423. Additionally, Facebook directed *Gowalla*'s decisions on the ongoing operations and availability of the *Gowalla* App.

424. While Facebook controlled, *Gowalla* it continued to offer the *Gowalla* App to consumer for at least three more months (until approximately March 2012). On information and belief, this activity was authorized, approved, managed and/or directed by Facebook, despite the known risk of harm from the continued deployment of the *Gowalla* App. Facebook eventually shuttered the *Gowalla* service and App around March 2012.

425. Accordingly, on information and belief Facebook knowingly managed and/or aided and abetted *Gowalla* in the commission of its wrongful activities described above and, consequently, is jointly and severally liable to the Plaintiffs on each of the claims and for all of the *Gowalla*-related harm and damages described herein.

426. On information and belief, Facebook's acquisition of *Gowalla* and/or substantially all of *Gowalla*'s staff, assets and operation was for less than equivalent value and via a transaction designed to improperly shield assets from *Gowalla*'s creditors. The transaction participants knowingly did not reserve sufficient assets to satisfy all creditor claims; *Gowalla* distributed substantially all consideration received from Facebook – which at the time was the predominant remaining assets of the business – to its equity-holders and management team for less than equivalent value and in a manner that left *Gowalla* insolvent. Accordingly, Facebook is *Gowalla*'s successor-in-interest and is liable on the claims asserted against *Gowalla*. The wrongfully distributed and/or transferred assets should also be impressed with a constructive trust to satisfy Plaintiffs' claims.

427. Facebook also acquired App Defendant Instagram for $300 million in cash and 23 million shares of Facebook stock. The parties announced that acquisition in April 2012 (roughly a month after the lead case was filed) and it closed on September 6, 2012.

Additional Common Allegations

428. Functionally, each of the identified Apps took control of the specified Plaintiffs' iDevices and without instruction from the Plaintiffs to do so, ran an I/O function that called up the iDevice's mobile address book, contemporaneously intercepted the responsive I/O communication containing the mobile address book information, initiated an Internet transmission that Plaintiffs never instructed their iDevices to make, and relayed, uploaded and publicly broadcast the intercepted mobile address book communication over the Internet, whereby the developer App Defendant for that App (and in the case of *Angry Birds Classsic* and *Cut the Rope*, defendant Chillingo) obtained the identified Plaintiffs' mobile address books (or substantial portions thereof). The transmissions were carried over Wi-Fi, 3G and the Internet to the developer App Defendant's servers. In the transmission process those private materials were publicly exposed to others via Wi-Fi and the Internet. This happened to Plaintiffs and, on information and belief, re-occurred on more than one occasion.

429. As a consequence, each developer App Defendant (and in the case of *Angry Birds Classic* and *Cut the Rope*, defendant Chillingo) obtained and was able to retain, keep, remotely store, and use at its discretion the identified Plaintiffs' private mobile address book materials and used Plaintiffs' iDevices to accomplish this unauthorized function without seeking (or obtaining) authorization to do so.

430. Plaintiffs were harmed by the Defendants' acts described above.

431. Defendants have benefited and were unjustly enriched by their wrongful acts.

432. Defendants' described acts were willful, intentional, knowing and malicious.

433. Defendants' described acts were reckless.

434. Because of the surreptitious nature of their actions – unobservable electronic thefts – only the Defendants know precisely what was stolen, when, and how from each Plaintiff or of the various uses that Defendants' made of Plaintiffs' private mobile address book materials.

435. Cryptographic hashing is a readily known, inexpensive technique commonly used in the computer and software industry, including to blind-match anonymized lists.

436. On information and belief, the Plaintiffs' mobile address books materials were not hashed by any App Defendants prior to February 2012 to protect Plaintiffs' privacy in advance of the unauthorized transmissions and uploads discussed above.

437. All described uploads, downloads, transmissions and communications constitute "electronic communications."

438. The App Defendants and their Apps exceeded any authorized access when they caused iDevices to transmit Plaintiffs' mobile address books elsewhere.

439. Each Defendant is a person.

440. Defendants' acts and wrongful conduct will continue unless enjoined by the Court.

441. Plaintiffs have no adequate remedy at law.

CLAIMS FOR RELIEF

442. Based on the foregoing allegations, Plaintiffs make the following claims for relief. As indicated at each cause of action below, each claim is asserted by various Plaintiffs on behalf of themselves and the applicable Class. Except as otherwise specifically indicated, each claim incorporates all of the allegations of this Complaint as if set forth fully therein.

Count I

Violations of the Unfair Competition Law (UCL)
California Business and Professions Code, § 17200, *et seq.*
(Against Apple, on Behalf of All Plaintiffs)[23]

443. Plaintiffs incorporate by reference allegations specific to each plaintiff in paragraphs 16 through 32 and the substantive allegations in paragraphs paragraphs 57 through 127.

444. In violation of California Business and Professions Code, §17200 et seq., ("Unfair Competition Law"), Apple's conduct in this regard is ongoing and includes, but is not limited to, statements made by Apple and Apple's omissions, including as set forth above.

445. Plaintiffs, on behalf of themselves and on behalf of each member of the Class, seek restitution, injunctive relief, and other relief allowed under the Unfair Competition Law.

446. Apple's business acts and practices are unlawful, in part, because they violate California Business and Professional Code, §1750, et seq., which prohibits false advertising, in that they were untrue and misleading statements relating to Apple's provision of goods and with the intent to induce consumers to enter into obligations relating to such goods, and regarding which statements Apple knew, or which by exercising reasonable care should have known, were untrue and misleading.

447. Apple's business acts and practices are also unlawful in that, as set forth herein, they violate the Consumer Legal Remedies Act, California Civil Code, §1750, et seq.

448. Plaintiffs reserve the right to identify additional provisions of the law violated by Apple as further investigation and discovery warrants.

449. Apple is therefore in violation of the unlawful prong of the Unfair Competition Law.

450. Apple's business acts and practices are also unfair because they have caused harm and injury-in-fact to Plaintiffs and members of the Class and for which Apple has no justification

[23] This claim was previously sustained by the Court with respect to Pirozzi. .

other than to increase, beyond what Apple would have otherwise realized, its market share and revenue from sale of the iDevices.

451. Apple's conduct lacks reasonable and legitimate justification in that it has benefited from such conduct and practices while Plaintiffs and members of the Class have been misled as to the nature and integrity of the iDevices and have lost money, including the purchase price of the iDevice and/or the difference of the inflated price and the price Apple should have charged for a product that fully disclosed the true nature of the iDevices.

452. Apple's conduct offends California public policy, the Consumer Legal Remedies Act, and/or the state constitutional right of privacy.

453. In addition, Apple's *modus operandi* constitutes a sharp practice in that Apple knew and should have known that consumers care about the status of personal information, privacy and property, but are unlikely to be aware or/and able to detect the means by which Apple and/or its licensors were conducting themselves in a manner adverse to its commitments and its users' interests. Apple is therefore in violation of the unfair prong of the Unfair Competition Law.

454. Apple's acts and practices were also fraudulent within the meaning of the UCL because they were likely to mislead members of the public.

455. While Apple represented at all times that the iDevices were safe and secure; in actuality, third party apps were able to access purchasers' private information without consent. Apple did not inform purchasers, like Plaintiffs, that their iDevices may be vulnerable to access by third parties, but instead, represented at all relevant times that Apple would not allow apps that steal user privacy into the App Store.

456. By engaging in the above-described acts and practices, Apple has committed one or more acts of unfair competition within the meaning of the UCL. Plaintiffs and members of the Class have suffered an injury-in-fact and have lost money and property, including, but not limited to, the expected utility and performance of their iDevices, the purchase price of their iDevices, and/or the difference between the price Class members paid and the actual worth of the product has Apple disclosed the true nature of the iDevices.

457. Apple had a duty to disclose the material privacy and security characteristics of the iDevices and their operations because (i) it knew or should have known about these characteristics at the time that Plaintiff and other members of the Class purchased their iDevices because Apple created the iDevices and the iOS that ran these devises, created the App Store, and reviewed each app available at the App Store; (ii) had exclusive knowledge of material facts that were not known to Plaintiffs; and (iii) made representations regarding the iDevices' protection of user privacy without disclosing that iDevices were not safe and that apps were capable of accessing private user data without consent.

458. Plaintiffs and members of the Class were deceived by Apple's representations, omissions, and cultivation of its reputation for security and privacy and reasonably relied on Apple's representations and omissions as described herein and were consequently injured as alleged herein.

459. Plaintiffs and members of the Class have suffered injuries as a direct and proximate result of Apple's unlawful, unfair and fraudulent business practices.

Count II

Additional Violations of the UCL

(*Against Apple on Behalf of the Opperman Plaintiffs*[24])

460. Apple's actions, as complained of herein, constitute unfair, deceptive, and/or unlawful practices committed in violation of the UCL.

461. In violation of California Business & Professions Code §§ 17200, et seq., Defendant Apple's conduct in this regard is ongoing and includes, but is not limited to, practices pertaining to iDevice and Apps.

462. By engaging in the acts and practices described herein, Defendant Apple has committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and Class Members have suffered injuries-in-fact and have lost money and/or property –

[24] The Opperman Plaintiffs are Beuershasen, Biondi, Dean, Dennis-Cooley, Green, Hodgins, Hoffman, King, Mandaywala, Moses, Paul, Sandiford and Varner.

specifically, money, valuable private mobile address books, private personal information, and exclusivity of control over their iDevices.

463. Plaintiffs purchased iDevices and obtained the identified Apps from Apple, resulting in the installation and activation of the App Defendants' App(s), with their identified harmful mobile address book functionalities, to be placed on their iDevices.

464. Apple engaged in unlawful business practices by, among other things:

a. Engaging in conduct, as alleged herein, that violates California Penal Code § 502;

b. Engaging in conduct, as alleged herein, that violates California Civil Code §§ 1750 *et seq.*, which seeks to protect consumers against unfair and sharp business practices and to promote a basic level of honesty and reliability in the marketplace;

c. Engaging in conduct, as alleged herein, that violates 18 U.S.C. §§ 1341, 2314 and 1961-1965.

d. Engaging in conduct, as alleged herein, that violates the federal Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C) and (a)(5).

e. Assisting in conduct, as alleged herein, that violates the Electronic Communications Privacy Act and corresponding state wiretap laws.

f. Engaging and/or assisting in conduct, as alleged herein, that violates Federal Trade Communications Act § 45.

Apple is therefore in violation of the "unlawful" prong of the UCL

465. Defendant Apple engaged in unfair business practices by, among other things:

a. Engaging in conduct where the utility of that conduct is outweighed by the gravity of the consequences to Plaintiffs and Class members;

b. Engaging in conduct that is immoral, unethical, unscrupulous, or substantially injurious to Plaintiffs and Class Members;

c. Engaging in conduct that undermines or violates the stated policies underlying the CLRA, which seeks to protect consumers against unfair and sharp business practices and to promote a basic level of honesty and reliability in the marketplace; and

d. Engaging in conduct that undermines or violates the stated policies underlying the federal and state statutes cited in the preceding section

466. In addition, Apple's modus operandi constitutes an unfair practice in two ways: (1) Apple knows, or should know, that consumers care about the content and control over their iDevices and the status of personal information, property and mobile communication privacy but are unlikely to be aware of the manner in which Defendants fail to fulfill their commitments to respect consumers' privacy and cause damage to consumers' property; and (2) to the extent that users do become aware of Defendants' conduct and practices, Apple's business models and practices are designed to shield wrongdoers from responsibility for adversely impacting consumers. Defendant Apple is therefore in violation of the "unfair" prong of the UCL.

467. Defendant Apple engaged in fraudulent business practices by engaging in conduct that was and is likely to deceive consumers acting reasonably under the circumstances. Defendant's fraudulent business practices include, but are not limited to:

a. Continuing to sell iDevices to consumers after actual awareness of the presence of iDevice flaws causing known harm to consumers, their property and their privacy.

b. Knowingly providing Apps to consumers after actual awareness of the presence in the Apps of non-compliant mobile address book-related computer contaminants and Trojan horse functionalities known to harm to consumers, their property and their privacy.

c. Engaging in false advertising and disseminating untrue and misleading statements relating to Apple's provision of goods and with the intent to induce consumers to enter into obligations relating to such goods, which statements Apple knew, or which by exercising reasonable care should have known, were untrue and misleading.

d. Promising, representing and advertising that consumers would receive a fully-functional App Store with their purchased iDevice[25] but instead providing consumers

[25] *Apple Introduces the New iPhone 3G*, Apple Press Info at http://www.apple.com/pr/library/2008/06/09Apple-Introduces-the-New-iPhone-3G.html (Apple June 9, 2008) ("Apple® today introduced the new iPhone™ 3G …[which] runs the incredible third party apps …iPhone 3G **includes** the new App Store, providing iPhone users with native applications in a variety of categories including games, business, news, sports, health, reference and travel. The App Store on iPhone works over cellular networks and Wi-Fi, which means it is

(including these Plaintiffs) iDevices with a locked App Store feature that did not allow immediate acquisition of Apps.

e. Breaching obligations of good faith and fair dealing to iDevice purchasers by requiring post-purchase relinquishment of promised economic benefits and submission to undisclosed transactions to receive the fully-functional App Store promised with a purchased iDevice.

f. Inserting unconscionable provisions into iDevice-related consumer agreements.

g. Failing to disclose the truth about known, harmful features of Apps that it provided to consumers, how they worked, and what they would do and concealing from consumers that the named Apps were malware (essentially Trojan horses) designed to, in part, non-consensually assume control of consumers' iDevices, relay consumers' mobile address books to the App developers' servers and allow App developers to obtain and keep consumers' mobile address books.

468. Defendant Apple is therefore in violation of the "deceptive" prong of the UCL.

469. As a direct and proximate result of Defendant Apple's unlawful, unfair, and fraudulent acts, business practices, and conduct, Plaintiffs and Class Members have suffered injury in fact and lost money as a result of Defendants' practices in that, among other things:

a. Plaintiffs lost the expected utility and performance of their iDevices, the purchase price of their iDevices, and/or the difference between the price Class members paid and the actual worth of the product had Apple disclosed the true nature of the iDevices.

b. Plaintiffs lost (i) the differential value between an iDevice with a fully-functional App Store versus an iDevice lacking or with a locked App Store, and/or (ii) the economic value of anything exchanged or given to secure a fully-functional App Store for Plaintiffs' iDevices.

---

accessible from just about anywhere, so you can purchase and download applications wirelessly and start using them instantly.")

c. Plaintiffs are forced to retain technicians to remove any vestiges of mobile address book-related malware from their iDevices and validate the integrity of their iDevices and data.

d. Plaintiffs lost the compensable value for the use of their iDevices and private mobile address books

470. All of the conduct alleged herein occurred in the course of Apple's business. Defendant's wrongful conduct was part of a pattern or generalized course of conduct repeated on tens of millions of occasions.

471. Apple had a duty to disclose the material features or absence of features that accompanied the iDevices (including the App Store) because (i) it knew or should have known about these characteristics at the time that Plaintiff and other members of the Class purchased their iDevices because Apple created, marketed and set the terms for sale for the iDevices and determined what features accompanied the iDevices; (ii) had exclusive knowledge of material facts that were not known to Plaintiffs; and (iii) made representations regarding the iDevices' features accompanying an iDevice purchase.

472. Plaintiffs, on behalf of themselves and each Class Member, seek restitution, injunctive relief, rescission, and other relief allowed under section 17200, et seq.

473. Apple financially benefited through its wrongful practices and increased, beyond what Apple would have otherwise realized, its market share and revenues from sale of the iDevices and on Apps.

474. It would be inequitable to permit Apple to retain its ill-gotten gains or the profits realized by engaging in this unlawful conduct.

475. Plaintiffs, on behalf of themselves and Class Members, seek restitution in the form of all Apple profits, valuation or unjustly obtained benefits and rescission of any unjustly obtained rights that may be attributable to this wrongful conduct.

476. Plaintiffs, on behalf of themselves and Class Members, seek disgorgement in the form of all Apple benefits and profits such as may be necessary to deter future violations of the unfair trade practice statute.

Count III
Violations of the California Unfair Competition Law ("UCL")
California Business & Professions Code §§ 17200, *et seq.*
(Against All App Defendants on Behalf of all Plaintiffs Except Pirozzi)

477. The App Defendants' actions, as complained of herein, constitute unfair, deceptive, and/or unlawful practices committed in violation of the UCL.

478. In violation of California Business & Professions Code §§ 17200, et seq., the App Defendants' conduct in this regard is ongoing and includes, but is not limited to, Defendants' information privacy and confidentiality practices.

479. By engaging in the above-described acts and practices, the App Defendants have committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and Class Members have suffered injury-in-fact and have lost money and/or property—specifically, valuable personal information.

480. Plaintiffs downloaded the App(s), which caused Defendants' App(s), with their functionality of downloading Plaintiffs' contact address book data, to be placed on their IDevices.

481. Defendants engaged in unlawful business practices by, among other things:

a. Engaging in conduct, as alleged herein, that violates California Penal Code § 502;

b. Engaging in conduct, as alleged herein, that violates California Civil Code §§ 1750 *et seq.*, which seeks to protect consumers against unfair and sharp business practices and to promote a basic level of honesty and reliability in the marketplace;

c. Engaging in conduct, as alleged herein, that violates Article I, Section 1 of the California Constitution; and

d. Engaging in conduct, as alleged herein, that violates the federal Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C) and (a)(5).

Defendants are therefore in violation of the "unlawful" prong of the UCL.

482. The App Defendants engaged in unfair business practices by, among other things:

a. Engaging in conduct where the utility of that conduct is outweighed by the gravity of the consequences to Plaintiffs and Class members;

b. Engaging in conduct that is immoral, unethical, unscrupulous, or substantially injurious to Plaintiffs and Class Members;

c. Engaging in conduct that undermines or violates the stated policies underlying the CLRA, which seeks to protect consumers against unfair and sharp business practices and to promote a basic level of honesty and reliability in the marketplace; and

d. Engaging in conduct that undermines or violates the stated policies underlying California Penal Code § 502; Article I, Section 1 of the California Constitution; and the federal Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C) and (a)(5).

e. In addition, Defendants' modus operandi constitutes an unfair practice in two ways: (1) Defendants know, or should know, that consumers care about the status of personal information and mobile communication privacy but are unlikely to be aware of the manner in which Defendants fail to fulfill their commitments to respect consumers' privacy; and (2) to the extent that users do become aware of Defendants' conduct and practices, Defendants' business models are designed to generate high traffic volume to make up for the loss of revenue from members disaffected by Defendants' misleading messages. Defendants *Instagram* and/or Path are therefore in violation of the "unfair" prong of the UCL.

483. The App Defendants engaged in fraudulent business practices by engaging in conduct that was and is likely to deceive consumers acting reasonably under the circumstances. Defendant's fraudulent business practices include, but are not limited to:

a. Failing to disclose the truth about what the Apps were, how they worked, and what they would do. What were portrayed as Apps to, for example, share pictures or play games, in fact, concealed what were essentially Trojan horses which engaged in surreptitious data collection practices immediately upon being downloaded upon a user's IDevice. Users who sought to obtain a photo sharing App ended up with a program on their IDevices that undertook actions that were never disclosed to IDevice users. Users were never informed that the Apps would make a copy of their contact address book, upload that address book to the App Defendants' servers, and that they would retain and use a copy of that secretly acquired information;

b. When the App Defendants represented that the App were "free," they were engaging in misrepresentations. The Apps were designed to hide the true price users would pay. In exchange for the Apps, users were required to relinquish a copy of their contact address book, a transaction to which they would not have permitted had they been informed of the truth about the real cost of the Apps;

c. When the App Defendants represented that the downloads were "free," they were engaging in misrepresentations. The downloads included within them a mechanism for extracting a price from the user (the user's contact address book). All of this was undisclosed and the user was not given all information necessary to fairly and honestly evaluate whether the App was really worth the download. Thus, the download was not free. The download was specifically designed to hide the fact that a price was being extracted from the user without the user's knowledge or consent. The App Defendants are therefore in violation of the "deceptive" prong of the UCL.

484. As a direct and proximate result of the App Defendants' unlawful, unfair, and fraudulent acts, business practices, and conduct, Plaintiffs and Class Members have suffered injury in fact and lost money as a result of Defendants' practices in that, among other things:

a. Plaintiffs lost any compensation for their investment of time, effort, skill, and creative energy used to build the user's unique contact address book, which has independent value as a result of the investment of time, effort, skill, and creative

energy by Plaintiffs and Class Members. The investment made by a user to create their contact address book is substantial and capable of valuation, based upon the time spent learning and building the contact address book, time spent creating and inputting data and information, the number of entries in the contact address book, and the time spent modifying and updating the contact address book.

b. Plaintiffs are forced to retain an expert in order to obtain removal of the Instagram and/or Path App(s) from their iDevices. The cost to hire a technician who can knowledgeably, effectively, completely, and permanently remove the Instagram and/or Path App(s), and all accompanying code, both disclosed and undisclosed, is substantial. The knowledge required from such an operation is not easily obtained outside of Apple itself. Thus, the false pretenses under which the app(s) were downloaded, installed, and run on the user's iDevices caused actual harm to users in necessitating expert removal of the app(s) and all related code, both disclosed and undisclosed, from the iDevice in order to restore the iDevice to its previously secure state.

485. All of the conduct alleged herein occurred in the course of Defendants' business. Defendants' wrongful conduct was part of a pattern or generalized course of conduct repeated on tens of millions of occasions.

486. Plaintiffs, on behalf of themselves and each Class Member, seek restitution, injunctive relief, rescission, and other relief allowed under section 17200, et seq.

487. On or about April 12, 2012, Instagram was purchased by Facebook for one billion dollars. This one billion dollar valuation was due, in whole or in part, to Instagram's theft and acquisition of tens of millions of user contact address books, which included hundreds of millions of names, email addresses, and telephone numbers. Instagram did not disclose to Apple Device owners that it was taking this information, and Instagram never compensated users for the taking of this data.

488. Similarly, the other App Defendants stole and acquired of tens of millions of user contact address books, which included hundreds of millions of names, email addresses, and

telephone numbers. The App Defendants did not disclose to iDevice owners that they were taking this information, and the App Defendants never compensated users for the taking of this data.

489. It would be inequitable to permit the App Defendants to retain their ill-gotten gains or the profits realized by engaging in this unlawful conduct.

490. Plaintiffs, on behalf of themselves and Class Members, seek restitution in the form of all Instagram and/or Path valuation that may be attributable to the App Defendants theft and acquisition of tens of millions of user contact address books.

491. Plaintiffs, on behalf of themselves and Class Members, seek disgorgement in the form of all App Defendants' benefits and profits such as may be necessary to deter future violations of the unfair trade practice statute.

Count IV
Violations of False and Misleading Advertising Law (FAL)
California Business & Professions Code § 17500, *et seq.*
***(Against Apple, on Behalf of All Plaintiffs)*[26]**

492. Plaintiffs incorporate by reference allegations specific to each plaintiff in paragraphs 16 through 32 and the substantive allegations in paragraphs paragraphs 57 through 127.

493. Plaintiffs and members of the Class have suffered injury in fact and have lost money or property as a result of Apple's violation of California Business & Professions Code §17500, *et seq*.

494. Apple's acts and practices as described herein have deceived and/or are likely to deceive members of the Class and the public. Apple has repeatedly advertised that its products were safe and secure. Apple has furthered assured consumers that it closely monitors the apps available in the App Store. Instead, Apple has left its customers vulnerable to unauthorized data breaches.

[26] This claim was previously sustained by the Court with respect to Pirozzi.

495. By its actions, Apple is disseminating uniform advertising concerning its products and services, which by its nature is unfair, deceptive, untrue, or misleading within the meaning of California Business & Professions Code §17500, et seq. Such advertisements are likely to deceive, and continue to deceive, the consuming public for the reasons detailed above.

496. The above-described false, misleading, and deceptive advertising Apple disseminated continues to have a likelihood to deceive in that Apple has failed to disclose that apps may be collecting (and downloading) confidential data such as contact information, location data, private photographs and videos on users' phones without consent.

497. In making and disseminating the statements alleged herein, Apple should have known its advertisements were untrue and misleading in violation of California Business & Professions Code §17500, et seq. Plaintiffs and members of the Class based their decisions to purchase the iDevice and/or purchase apps through the App Store in substantial part on Apple's misrepresentations and omitted material facts. The revenues to Apple attributable to products sold in those false and misleading advertisements amount to millions of dollars. Plaintiffs and the Class were injured in fact and lost money or property as a result.

498. The misrepresentations and non-disclosures by Apple of the material facts detailed above constitute false and misleading advertising and therefore constitute a violation of California Business & Professions Code § 17500, et seq.

499. As a result of Apple's wrongful conduct, Plaintiffs and the Class request that this Court enjoin Apple from continuing to violate California Business & Professions Code § 17500, et seq.

Count V
Additional Violations of the FAL
(*Against Apple, on Behalf of the Opperman Plaintiffs*)

500. Plaintiffs and Class members suffered injury in fact and lost money or property as a result of Apple's violation of California Business & Professions Code §17500, *et seq*.

501. Apple's acts and practices described herein have deceived and/or are likely to deceive members of the Class and the public. In addition to the above-described ads, Apple has repeatedly and broadly advertised its iDevices as including a functional App Store, which it does

not upon purchase. Apple has furthered assured consumers that "sandboxing" provides security and privacy protection for the Contacts database and users' private mobile address books when in fact it does not.

502. By its actions, Apple is disseminating uniform advertising concerning its products and services, which by its nature is unfair, deceptive, untrue, or misleading within the meaning of California Business & Professions Code §17500, et seq. Such advertisements are likely to deceive, and continue to deceive, the consuming public for the reasons detailed above.

503. The above-described false, misleading, and deceptive advertising Apple disseminated continues to have a likelihood to deceive in that Apple has failed to disclose that iDevices do not contain a fully-functional App Store or what would be required to obtain one, and that iDevices non-consensually disclose, disseminate and relay iDevice owners' mobile address books to third parties as a result of Apps provided by Apple and others.

504. In making and disseminating the statements alleged herein, Apple should have known its advertisements were untrue and misleading in violation of California Business & Professions Code §17500, et seq. Plaintiffs and members of the Class based their decisions to purchase the iDevice and/or purchase apps through the App Store in substantial part on Apple's misrepresentations and omitted material facts. The revenues to Apple attributable to products sold in those false and misleading advertisements amount to millions of dollars. Plaintiffs and the Class were injured in fact and lost money or property as a result.

505. The misrepresentations and non-disclosures by Apple of the material facts detailed above constitute false and misleading advertising and therefore constitute a violation of California Business & Professions Code § 17500, et seq.

506. As a result of Apple's wrongful conduct, Plaintiffs and the Class request that this Court enjoin Apple from continuing to violate California Business & Professions Code § 17500, et seq.

Count VI
Violations of the Consumer Legal Remedies Act (CLRA), California Civil Code, §1750, *et seq.*
(Against Apple, on Behalf of All Plaintiffs)[27]

507. Plaintiffs incorporate by reference allegations specific to each plaintiff in paragraphs 16 through 32 and the substantive allegations in paragraphs paragraphs 57 through 127.

508. In violation of Civil Code, §1750, et seq., Apple has engaged and is engaging in unfair and deceptive acts and practices in the course of transactions with Plaintiff, and such transactions are intended to and have resulted in sales of any merchandise.

509. In violation of the CLRA, Apple has engaged, and is engaging, in unfair and deceptive acts and practices in the course of transaction with Plaintiff, and such transactions are intended to and have resulted in the sale of goods to consumers.

510. Plaintiffs and members of the Class are consumers as that term is used in the CLRA Act because they sought or acquired Apple's goods (the iDevices) for personal, family, or household purposes. Apple's past and ongoing acts and practices include but are not limited to: Apple's representations that its goods were of a particular standard, quality, and grade, when in fact, they were of another, in violation of Civil Code, §1770(a)(7).

511. Specifically, as described herein, Apple has made the following representations, expressly or by implication to Plaintiffs and other members of the Class about the iDevices: (i) that Apple designed the iDevices to safely and reliably download third party apps, (ii) that the App Store does not permit apps that violate its developer guidelines (including apps that contain pornography, violate user privacy, and hog bandwidth) to be sold or to be made available for free through the App Store, (iii) that "Apple takes precautions – including administrative, technical, and physical measures – to safeguard [purchaser's] personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction;" (iv) that

[27] This claim was previously sustained by the Court with respect to Pirozzi.

Apple does not allow one app to access data stored by another app; and (v) that Apple does not allow an app to transmit/upload/download data from iDevices without the user's consent.

512. These representations were materially misleading.

513. Plaintiffs and members of the Class would not have purchased the iDevices and/or would not have paid as much for them if Apple disclosed that the above representations were false and if there were aware that third party apps can obtain personal information from the iDevices without users' consent.

514. Apple's violations of the CLRA have caused damage to Plaintiffs and the other Class members and threaten additional injury if the violations continue. This damage includes the injuries and losses set forth above.

515. Under §1782 of the CLRA, Apple has received notice in writing by certified mail of the particular violations of §1770 of the CLRA from Plaintiffs on behalf of all Class members, demanding Defendant offer to resolve the problems associated with the actions detailed above and give notice to all affected consumers of the intent to so act.

516. Thirty days have passed since Plaintiffs sent their CLRA letters, registered mail return receipt requested, and Apple has failed to take the actions required by the CLRA on behalf of all affected consumers. Plaintiffs and the Class are therefore entitled to all forms of relief provided under § 1780 of the CLRA.

517. Based on its knowledge or reckless disregard of the facts as detailed herein, Apple was guilty of acting with malice, oppression or fraud.

Count VII
Additional CLRA Claims
(*Against Apple, on Behalf of the Opperman Plaintiffs*)

518. In violation of the CLRA (Civil Code, §1750, et seq.), Apple has engaged and is engaging in unfair and deceptive acts and practices in the course of transactions with the Plaintiffs, and such transactions are intended to and have resulted in sales of merchandise.

519. Plaintiffs and members of the Class are consumers under the CLRA Act. Each sought or acquired Apple's goods (the iDevices) for personal, family, or household purposes.

520. Apple's past and ongoing acts and practices in violation of the CLRA include but are not limited to: (i) §1770(a)(5), (7), (9) and (16) in that Apple represented that the iDevices and Apple's associated services have characteristics, uses and benefits they do not have; were of a particular standard, quality and grade, but were in fact not; that they had been supplied in accordance with previous representations when they had not; and in that Apple advertised and sold iDevices with the intent not to sell them as advertised. In particular, Apple falsely represented that iDevices were highly secure, "sandboxed," and accompanied by a fully-functioning App Store with immediate access to Apps, that the add-on component Apps available in the App Store were not harmful, malicious or violative of user privacy, that the App Store was appropriately curated, and that Apple would not allow malicious Apps or Apps that invade iDevice owner's privacy to be available via the App Store; (ii) §1770(a)(14) and (17) in that Apple advertised the purchase and acquisition of iDevices and Apple's associated services as conferring or involving rights, remedies and economic benefits (a functional App Store and App access) that did not accompany the purchase of an iDevice but the earning of that benefit was instead made contingent on an additional undisclosed subsequent post-purchase transaction mandated by Apple; and (c) §1770(a)(19) in that Apple included unconscionable provisions in iDevice-associated consumer agreements.

521. Specifically, as described herein, Apple has made the forgoing and following representations, expressly or by implication to Plaintiffs and other members of the Class about the iDevices and associated services: (i) that a functional App Store and immediate App access accompanied iDevice purchases.

522. These representations were materially misleading.

523. Apple marketed the App Store and iDevice in myriad national ad campaigns as a valuable, included fully functional component feature of each iDevice. Plaintiffs saw such ads. Plaintiffs and members of the Class would not have purchased the iDevices and/or would not have paid as much for them if Apple disclosed that the above representations were false.

524. Plaintiffs would not have accepted the following apps from Apple or the App Store had Apple truthfully represented that they contained computer contaminants that would adversely impact their private mobile address books: *Angry Birds Classic* and *Cut the Rope* (both containing the integrated *Crystal* platform), *Foodspotting, Foursquare, Gowalla, Hipster, Instagram, Kik Messenger, Path, Twitter,* and *Yelp!*.

525. Apple's violations of the CLRA have caused damage to Plaintiffs and the other Class members and threaten additional injury if the violations continue. This damage includes the injuries and losses set forth above.

526. Under §1782 of the CLRA, Apple has received notice in writing by certified mail of the particular violations of §1770 of the CLRA from Plaintiffs on behalf of all Class members, demanding Defendant offer to resolve the problems associated with the actions detailed above and give notice to all affected consumers of the intent to so act.

527. Thirty days have passed since Plaintiffs sent their CLRA letters, registered mail return receipt requested, and Apple has failed to take the actions required by the CLRA on behalf of all affected consumers. Plaintiffs and the Class are therefore entitled to all forms of relief provided under § 1780 of the CLRA.

528. Plaintiffs have or will contemporaneously file an affidavit on these violations.

529. Based on its knowledge or reckless disregard of the facts as detailed herein, Apple was guilty of acting with malice, oppression or fraud.

Count VIII
Negligent Misrepresentation

(*Against Apple on Behalf of All Plaintiffs*[28])

530. Plaintiffs incorporate by reference allegations specific to each plaintiff in paragraphs 16 through 32 and the substantive allegations in paragraphs paragraphs 57 through 127.

[28] This claim was previously sustained by the Court with respect to Pirozzi.

531. Apple claims to review each application before offering it to its users, purports to have implemented app privacy standards, and claims to have created a strong privacy protection for its customers.

532. However, unbeknownst to consumers such as Plaintiffs, Apple failed to properly monitor app makers and to safeguard Plaintiffs' private information. In making these representations to Plaintiffs and the Class, Apple intended to induce Plaintiffs and the Class to purchase the iDevices and to obtain apps through the App Store.

533. At all times herein, Plaintiffs and the Class were unaware of the falsity of Apple's statements. Plaintiff and the Class reasonably acted in response to the statements made by Apple when they purchased an iDevice and downloaded apps from the App Store.

534. As a proximate result of Apple's negligent misrepresentations, Plaintiffs and Class members purchased an iDevice and downloaded apps from the App Store.

Count IX

Negligent Misrepresentation

(*Against Apple on Behalf of the Opperman Plaintiffs*)

535. Apple's and the App Defendants' representations described herein were not true.

536. In making these representations to Plaintiffs and the Class, Apple intended to induce Plaintiffs and the Class to purchase iDevices, to use them in their intended manner and to obtain and accept apps from Apple, the App Store and the App Defendants.

537. At all times herein, Plaintiffs and the Class were unaware of the falsity of Apple's and the App Defendants' statements. Plaintiff and the Class reasonably acted in response to the statements made by Apple and the App Defendants when they purchased iDevices and obtained and accepted the App Defendants' apps from the App Store.

538. As a proximate result of Apple's and the App Defendants' negligent misrepresentations, Plaintiffs and Class members purchased an iDevice, obtained and accepted apps from the App Store, including those of these App Defendants, and suffered harm thereby.

Count X

Violations of California's Computer Crime Law (*"CCL"*), Cal. Pen. Code § 502 (*Against All Defendants on Behalf of all Plaintiffs Except Pirozzi*) [29]

539. The App Defendants violated *CCL* subsections 1, 2, 6, 7 and 8. Cal. Pen. Code §§ 502(c)(1), (2), (6), (7), (8). The *CCL* imposes civil liability upon any person who:

> (1) "Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data," *id*. § 502(c)(1);
>
> (2) "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, … whether existing or residing internal or external to a computer, computer system, or computer network," *id*. § 502(c)(2);
>
> (3) "Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section," *id*. § 502(c)(6);
>
> (4) "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network," *id*. § 502(c)(7); or,
>
> (5) "Knowingly introduces any computer contaminant into any computer, computer system, or computer network." *id*. § 502(c)(8).

540. Plaintiffs' iDevices are computers under the *CCL*.

541. Plaintiffs' mobile address books and the contacts, fields and data points therein constitute data under the *CCL*.

542. The *CCL* defines "Computer Contaminant" as meaning "any set of computer instructions that are designed to…. record, or transmit information within a computer, computers system, or computer network without the intent or permission of the owner of the information." California Penal Code § 502(b)(10)

543. Each App Defendant's identified App contained a set of instructions or codes to trigger an iDevice to transmit within itself and upload to the Internet and transmit from identified Plaintiffs' iDevice substantial portions of the iDevice's mobile address book without a correlating subroutine or instruction set requesting advanced permission from or alerting the iDevice owner.

544. Plaintiffs did not give permission for or intend for these transmissions of their

[29] Plaintiffs Arabian and Carter bring claims under this Count against Defendants Instagram and Path, respectively, and do not assert claims under this Count against Defendant Apple.

mobile address book data to occur.

545. Accordingly, each such set of instructions or codes in each App Defendant's identified App is a computer contaminant under the *CCL*.

546. The App Defendants built their respective identified Apps and had knowledge of their contents, including the instructions or codes constituting computer contaminants that resided therein.

547. Apple thorough reviewed each of the identified Apps and had knowledge of their contents, including the instructions or codes constituting computer contaminants that resided therein.

548. Apple and each App Defendant knowingly introduced those instructions and codes into Plaintiffs' iDevices when they transmitted and deployed the App Defendants' Apps onto the identified Plaintiffs' iDevices. Accordingly, Apple and each App Defendant violated *CCL* § 502(c)(8).

549. Each App Defendant has violated *CCL* § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the iDevices of Plaintiffs and Class Members, which transmitted the contact address book to Defendants' servers

550. As a result of the computer contaminants contained therein, each App Defendants' App constitutes "a means of accessing a computer, computer system, or computer network in violation of" the *CCL*. The App Defendants and Apple provided and assisted in providing those means (i.e., the Apps). Accordingly, Apple and each App Defendant violated *CCL* § 502(c)(6).

551. Each App Defendant has violated *CCL* § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and Class Members' iDevices, in particular, their contact address book data.

552. Each App Defendant knowingly accessed the iDevice mobile address book of each Plaintiff identified to have that App Defendant's App, used without permission that mobile address book data and iDevice and thereby wrongfully controlled and obtained that mobile address book data and mobile address book property. Plaintiffs did not grant the App Defendants permission to

use that data. Accordingly, Apple and each App Defendant violated *CCL* § 502(c)(1).

553. Each App Defendant has violated California Penal Code § 502(c)(1) by knowingly and without permission, altering and making use of data from Plaintiffs' and Class Members' iDevices in order to execute a scheme to defraud consumers into registering as *Instagram* and/or Path users, and to wrongfully obtain valuable private data from Plaintiffs and Class Members.

554. Each App Defendants has violated California Penal Code § 502(c)(1) by knowingly and without permission, altering and making use of data from Plaintiffs' and Class Members' iDevices in order to: (1) deceive Plaintiffs and Class Members into surrendering unknowing control over their contact address book and the information contained therein for Defendants' financial gain; and (2) deceive Plaintiffs and Class Members into accepting, downloading, and using the App(s) that contained undisclosed code that would circumvent protections on the iDevices that were designed to keep information therein safe, secure, and private.

555. App Defendants' conduct was also part of a scheme or artifice to deceive or defraud Plaintiffs in violation of *CCL* § 502(c)(1) and obtain their mobile address book data.

556. Each App Defendant also knowingly copied and took mobile address book data residing on each identified Plaintiffs' iDevice. Again, this was without any Plaintiffs' permission. Accordingly, each App Defendant violated *CCL* § 502(c)(2).

557. Each App Defendant has violated California Penal Code § 502(c)(2) by knowingly and without permission, accessing and taking data from Plaintiffs' and Class Members' iDevices.

558. Each App Defendant's access of Plaintiffs' and the Class members' iDevices to "scrape" Plaintiffs' and Class members' private mobile address book materials was in violation of the Apple IDPLA and SDK agreements and, thus, was without permission. Accordingly, each App Defendant violated *CCL* § 502(c)(7).

559. Each App Defendant has violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' and Class Members' iDevices, in particular, their contact address book data.

560. Under the CCL, "a person who causes, by any means, the access of a computer,

computers system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Cal. Pen. Code §502(j).

561. The App Defendants copied, used, made use of, interfered with, and/or altered data belonging to Plaintiffs and the Class members (1) in and from the state of California; (2) in the home states of Plaintiffs and Class members; (3) in the states in which the servers that provided the communication link between Plaintiffs and the App(s) were located, and (4) in the states in which the servers that stored information obtained from Plaintiffs and Class Members were located. The identified Apps, which at least in part caused the access of Plaintiffs' iDevices, were transmitted to Plaintiffs iDevices from California. Accordingly, Plaintiffs' iDevices are deemed to have been accessed in California, in the state of each Plaintiff's residence and in the state or locale in which each Defendant's servers are located.

562. As a direct and proximate cause of Apple and the App Defendants' unlawful conduct within the meaning of *CCL* § 502, Apple and the App Defendants have caused loss and damage to Plaintiffs and the Class Members in an amount to be proven at trial.

563. Plaintiffs and the Class members are entitled to recover no less than the reasonable and necessary expense or cost for a technician or information technology professional to verify that their iDevices, mobile address books, and other data were not altered, damaged, corrupted or deleted by the Defendants' wrongful access to them and any additional costs necessary to restore or repair any alteration, damage, corruption or deletion. (Estimates for such services indicate that they can take as much as twenty hours at a costs of up to $250 per hour, which would be a total cost of in excess of $10,000 per wireless mobile device.)

564. Plaintiffs and Class members seek compensatory damages in an amount to be proven at trial, and injunctive or other equitable relief.

565. Plaintiffs lost any compensation for their investment of time, effort, skill, and creative energy used to build the user's unique contact address book, which has independent value as a result of the investment of time, effort, skill, and creative energy by Plaintiffs and Class

Members. The investment made by a user to create their contact address book is substantial and capable of valuation, based upon the time spent learning and building the contact address book, the time spent creating and inputting data and information, the number of entries in the contact address book, and time spent modifying and updating the contact address book.

566. Plaintiffs and Class members have suffered irreparable injury from those unauthorized acts, notably, the public exposure of and the Defendants' wrongful acquisition of their private and sensitive mobile address book information, leading to a continuing threat of exposure and injury for which Plaintiffs have no adequate remedy at law, entitling Plaintiffs and Class Members to injunctive relief.

567. Plaintiffs and Class Members have suffered irreparable and incalculable harm and injuries from Defendants' violations. The harm will continue unless the App Defendants and Apple are enjoined from further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

568. Plaintiffs and Class members are entitled to punitive damages under California Penal Code § 502(e)(4) because App Defendants' violations were willful, and, upon information and belief, App Defendants are guilty of oppression, fraud, or malice as defined by California Civil Code §3294.

569. Plaintiffs and Class Members are also entitled to recover their reasonable attorneys' fees under Cal. Penal Code §502(e).

Count XI
Violations of Federal Computer Fraud & Abuse Act
18 U.S.C. §§ 1030(a)(2)(C), (a)(5) & (g)
(*Against all App Defendants on Behalf of all Plaintiffs Except Pirozzi*)

570. Plaintiffs' devices are "protected computers."

571. Plaintiffs and Class Members have used their iDevices in interstate and/or foreign commerce.

572. The aggregate loss in any one-year period exceeds $5,000.

573. The App Defendants' acts and the unauthorized mobile address book transmissions jeopardized public security and computers owned or used by the government in furtherance of

justice, defense, or security.

574. On the basis of the defendants' above alleged actions, the App Defendants have each violated the requisite sections of 18 U.S.C. § 1030 so as to subject them under 18 U.S.C. § 1030(g) and to permit recovery in a civil action by any person who suffers damage or loss by reason of the violation.

575. Each App Defendant has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

576. Each App Defendants has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(i), by knowingly causing the transmission of a program, information, code, or command and as a result causing a loss to one or more persons during any one-year period aggregating at least $5000 in value.

577. Each App Defendant had the requisite intent to defraud.

578. On information and belief, these App Defendants' conduct has been intentional and willful in nature.

579. As described herein, each of the App Defendants inserted code or instructions into their Apps that surreptitiously harvested Plaintiffs' and Class members' mobile address books. Apple, as a result of its thorough review process, knew of this.

580. These Defendants had no authorization to take or store this valuable information, and each acted intentionally.

581. Plaintiffs have suffered damage and/or loss by reason of each of these Defendants' violations of 18 U.S.C. § 1030.

582. Plaintiffs and Class Members lost any compensation for their investment of time, effort, skill, and creative energy used to build the user's unique contact address book, which has independent value as a result of the investment of time, effort, skill, and creative energy by Plaintiffs and Class Members. The investment made by a user to create their contact address book

is substantial and capable of valuation, based upon the time spent learning and building the contact address book, the time spent creating and inputting data and information, the number of entries in the contact address book, and time spent modifying and updating the contact address book.

583. Plaintiffs and Class Members are forced to retain an expert in order to obtain removal of the identified App(s) from their iDevices. The costs to hire a technician who can knowledgeably, effectively, completely, and permanently remove the App(s) and all related code, both disclosed and undisclosed, is substantial. The knowledge required from such an operation is not easily obtained outside of Apple itself. Thus, the false pretenses under which the App(s) were downloaded, installed, and run on the user's iDevice caused actual harm to users in necessitating expert removal of the App(s) and all related code, both disclosed and undisclosed, from the iDevice in order to restore the iDevice to its previously secure state.

584. Plaintiffs and Class Members have suffered loss by reason of these violations.

585. As a consequence, Plaintiffs and the Class members have suffered aggregate losses in a one year period above $5,000.

586. Plaintiffs seek recovery of their compensatory damages as authorized under 18 U.S.C. § 1030(g), including: (i) reasonable costs for validating the integrity of the Plaintiffs' mobile address books and/or restoring such address books to the condition they were in before the Defendants' respective offenses; (ii) costs for appropriate additional security measures on the Plaintiffs' iDevices to remedy the "Contacts" feature and mobile address book-related security flaws (and to inhibit and prevent similar offenses in the future); (iii) the reasonable costs for each Plaintiff to conduct or have conducted a detailed damage and integrity assessment of his or her iDevice and their mobile address books maintained thereon and to assess whether the mobile address books and/or its availability or accessibility or the iDevice device has been impaired in any way; and (iv) the a daily iDevice rental rate or the value and costs of the wireless airtime that those Apps caused to be consumed while surreptitiously uploading any portion of a Plaintiff's address books from his or her iDevice.

587. Each App Defendant's conduct similarly affected and caused the losses described

above to many thousands to millions of users.

588. The App Defendants' unlawful access to Plaintiffs' and Class Members' computers and computer communications also have caused Plaintiffs and Class Members irreparable injury. Unless restrained and enjoined, the App Defendants will continue to commit such acts. Plaintiffs' and Class Members' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiffs and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

Count XII
Violations of the ECPA, 18 U.S.C. § 2510, *et seq*.
(*Against all App Defendants on Behalf of all Plaintiffs Except Pirozzi*)

589. The ECPA, 18 U.S.C. § 2510 *et seq.*, makes it unlawful for a person to intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any wire, oral, or electronic communication within the meaning of 18 U.S.C. § 2511(1).

590. Each App Defendant is a person covered by section 2511's prohibition on interceptions because they are corporations. 18 U.S.C. § 2510(6).

591. Each App Defendant violated 18 U.S.C. § 2511 by intentionally intercepting and procuring Plaintiffs' and Class Members' electronic communications, without Plaintiffs' or Class Members' direct or indirect, express or implied, knowledge, consent, or authorization.

592. Under the ECPA, an "interception" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The ECPA does *not* require a contemporaneous acquisition, rather it requires that Defendants "acqui[re] . . . the contents of any . . . electronic . . . communication." *Id.* Each App Defendant acquired the contents of Plaintiffs' and Class Members' contact address books, in violation of the ECPA. To the extent that contemporaneity is required, it is met here because Plaintiffs and Class Members downloaded the App Defendants' app(s) and, upon using the app(s), the secret code triggers the contemporaneous interception of Plaintiffs' and Class Members' contact address books.

593. At all relevant times, each App Defendant engaged in business practices of

intercepting and procuring Plaintiffs' and Class Members' electronic communications, which included procuring users' contact address books from their iDevices. Once each App Defendant obtained these electronic communications, including address book data, they used such to aggregate iDevice data of Plaintiffs and Class Members as they used their iDevices. Thus, each App Defendant acquired the substance, purport, meaning, or contents of those communications through the use of an electronic, mechanical, or other device.

594. The contents of data transmissions to and from Plaintiffs' and Class Members' iDevices constitute "electronic communications" within the meaning of 18 U.S.C. § 2510. Moreover, Plaintiffs' and Class Members' address book data are "electronic communications" under the ECPA, because they constitute "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part . . . ." 18 U.S.C. § 2510(12). In addition, each App Defendant's respective App (and any components provided by Chillingo) used to transfer information constitutes alone, and in combination with an iDevice, an "electronic device" under 18 U.S.C. § 2510(5) and all other relevant federal and state statutes cited herein

595. Plaintiffs and Class Members are "person[s] whose . . . electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter," within the meaning of 18 U.S.C. § 2520.

596. To intercept the contents of the electronic communications transmitted while Plaintiffs and Class Members used the App Defendants' app(s), each App Defendant made use of special software code specifically designed to collect and contemporaneously transmit the users' contact address book data. Plaintiffs' and Class Members' electronic communications derived from their activities in downloading and using the App Defendants' app(s). Plaintiffs' and Class Members' activity on the App Defendants' app(s) constituted electronic communications under 18 U.S.C. § 2510(12) because they were the transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce. In addition, the App Defendants' apps individually, and in combination with an iDevice, constitute "electronic

devices" under 18 U.S.C. § 2510(5).

597. Each App Defendant intercepted Plaintiffs' and Class Members' electronic communications contemporaneously with their transmission to and/or from the users' iDevices. Each App thus took control of the iDevice and, without instruction from a Plaintiff to do so, ran an I/O function that called up the iDevice's mobile address book, contemporaneously intercepted the responsive I/O communication containing mobile address book information, initiated an Internet transmission that Plaintiffs never instructed their iDevices to make, and relayed and publicly broadcast the intercepted mobile address book communication over the Internet, whereby the App Defendant obtained Plaintiffs' mobile address books (or substantial portions thereof). The transmission was carried via Wi-Fi, 3G, and the Internet to each App Defendant's servers. In the process, the user's private address book materials were publicly exposed to others via Wi-Fi and the Internet.

598. In other words, the App Defendants' apps contained hidden code which, unknown to the user, triggered upon the download and use of the app. When a user downloaded and used the App Defendants' app(s), the app(s) automatically, employing the embedded code hidden within them, ran a function that called up the iDevice's mobile address book and sent a copy of its contents to the App Defendant's servers. At that point, the user triggered the App Defendants' app(s) for some use and generated an electronic communication, the calling up of the contact address books, which the App Defendants intercepted contemporaneously and sent to their respective servers.

599. Each App Defendant employed computer contaminants in their respective Apps to contemporaneously intercept, then use, iDevice processor I/O communications containing Plaintiffs' mobile address book materials. As a direct result of these interceptions, the App Defendants obtained information consisting of material portions of Plaintiffs' mobile address books.

600. Each App Defendant was not the intended recipient of the Internet transmissions containing the material portions of Plaintiffs' mobile address books that originated from their iDevices. Plaintiffs—as the owners of those iDevices—have sole authority and discretion to initiate

an approved communication or transmission and to designate who is (or is not) an intended recipient of a communication issuing from his or her iDevice. Plaintiffs never authorized or intended those described Internet transmissions and, thus, did not designate or intend for the App Defendants to be recipients of the transmissions or the information contained therein. Thus, as alleged herein, each App Defendant has also, without authorization, intentionally and contemporaneously intercepted electronic communications (i.e., the iDevice Internet transmissions) that contained some or all of the private mobile address book materials from Plaintiffs' iDevices and has intentionally made use of the content of such communications.

601. Each App Defendant violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting and endeavoring to intercept Plaintiffs' and Class Members' wire and/or electronic communications to, from, and within their iDevices.

602. Each App Defendant violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing and endeavoring to disclose to another person the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and Class Members' electronic communications.

603. Each App Defendant violated 18 U.S.C. § 2511(1)(d) by intentionally using and endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and Class Members' electronic communications.

604. Each App Defendant's intentional interception of these electronic communications without Plaintiffs' or Class Members' knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

605. Each App Defendant intentionally used such electronic communications, with knowledge, or having reason to know, that the electronic communications were obtained through interception, for an unlawful purpose.

606. Each App Defendant unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability, revenue, and user base.

This disclosure was not necessary for the operation of the App Defendants' systems or to protect the App Defendants' rights or property.

607. Section 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

608. Each App Defendant is liable directly and/or vicariously for this cause of action. Plaintiffs and Class Members therefore seek remedies as provided by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with section 2520(c) to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fee and other litigation costs reasonably incurred.

609. Plaintiffs and Class Members, pursuant to 18 U.S.C. § 2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 for each day of violation, actual and punitive damages, reasonable attorney's fees, and each App Defendant's profits obtained from the above-described violations. Unless restrained and enjoined, the App Defendants will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate them for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided under 18 U.S.C. § 2520.

Count XIII
Violation of the California Wire Tap/
Invasion of Privacy Act, Cal. Pen. Code § 630, *et seq*.
(*Against Foodspotting, Instagram, Path, Twitter and Yelp on Behalf of the CAD Plaintiffs*[30])

610. On information and belief, the computer systems and servers of the following California-headquartered App Defendants ("CADs'") are located in California: Foodspotting, *Instagram*, Path, Twitter and Yelp.

611. On information and belief, the unauthorized CAD-associated transmissions of Plaintiffs' address book materials resulted, in whole or in part, in the CAD Plaintiffs' mobile address book materials being electronically transmitted within California and, on information and

[30] The "CAD Plaintiffs" are plaintiffs who downloaded the *Foodspotting, Instagram, Path, Twitter* and *Yelp* apps.

belief, within the CADs' computer systems and outsourced systems located in California.

612. Accordingly, Plaintiffs are entitled to the benefits and protection of and the CADs are subject to the California's Wiretap/Invasion of Privacy Act, Cal. Pen. Code § 631.

613. The CADs were not intended recipients of the Plaintiffs' iDevices' self-actuated CAD-directed transmissions, which occurred without Plaintiffs' authorizations.

614. The CADs willfully and without Plaintiffs' consent read, or attempted to read, or to learn the contents of such unauthorized mobile address book transmissions while they were in transit over the Internet or being received within California, learned such contents and made use of the contents of such communications, all without the consent of the Plaintiffs.

615. The CAD's accessing of the communications containing Plaintiffs' mobile address books or substantial portions thereof was without authorization or consent.

616. Communications from the CADs to the Plaintiffs iDevices (i.e., electronic "handshakes") were sent from California. Communications from Plaintiffs' iDevices were received by the CADs and sent to California.

617. Plaintiffs did not consent to any of the CAD's actions in furtherance of the interception or use of their mobile address book communications.

618. None of the CADs is a "public utility engaged in the business of providing communications services and facilities…" and the actions alleged herein by the CADs were not undertaken "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

619. The activities conducted by the CADs were not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

620. The CADs directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiffs and California-based web entities.

621. Accordingly, the CAD Defendants Foodspotting, *Instagram*, Path, Twitter and Yelp!, have willfully violated Cal. Pen. Code § 631.

622. The CAD Plaintiffs have suffered loss and damage, as discussed herein, by reason of these violations, including, without limitation, violations and deprivations of their property rights and right of privacy in their mobile address books.

623. The CAD Defendants' actions were outrageous.

624. Unless restrained and enjoined, the CADs will continue to commit such acts. Under Section 637.2 of the California Penal Code, Plaintiffs have been injured by the violations of California Penal Code section 631 and are entitled to damages and injunctive relief.

Count XIV
Violations of the Texas Wiretap Acts[31]
(*Against all App Defendants on Behalf of the Texas Plaintiffs*[32])

625. Each Defendant's App constitutes an "electronic, mechanical or other device" within the meaning of TEX. CODE CRIM. PROC. art. 18.20, § 1(3) and TEX. PEN. CODE § 16.02(a).

626. The App Defendants intentionally intercepted, disclosed and/or used the contents of electronic communications containing Plaintiffs' address book materials.

627. Plaintiffs were harmed by the App Defendants' conduct allege herein, and Plaintiffs seek statutorily available damages.

Count XV
Invasion of Privacy (Intrusion upon Seclusion)
(*Against All App Defendants on Behalf of the Opperman Plaintiffs*)

628. Plaintiffs have reasonable expectations of privacy in their iDevices and their mobile address books.

629. The Plaintiffs' private affairs include the contents of their iDevices, their private mobile address books, and those address books' unique contacts and fields, which identify persons with whom Plaintiffs associate and communicate. These are not matters of legitimate public concern.

---

[31] *See also* CAL. PENAL CODE § 502(e)(1) (authorizing a civil recovery of compensatory damages for the unauthorized access, copying or use of another's computer or computer data) and § 637.2 (authorizing civil actions for each victim of eavesdropping or wire tapping under CAL. PENAL CODE §§ 631 or 632 to recover from the violator a monetary award of ***the greater of*** $5,000 or three times actual damages).

[32] The Texas Plaintiffs are Beuershasen, Biondi, Dean, Hodgins, Hoffman, King and Varner.

630. By surreptitiously obtaining, improperly gaining knowledge, reviewing and retaining Plaintiffs' private mobile address books (or substantial portions thereof), the App Defendants intentionally intruded on and into each respective Plaintiff's solitude, seclusion or private affairs.

631. The App Defendants intrusions were highly offensive to a reasonable person. These intrusions were so highly offensive that myriad newspaper articles, blogs, op eds., and investigative exposes' were written complaining and objecting vehemently to these defendants' practices, Congressional inquiries were opened to investigate these practices and some defendants even publicly apologized. The surreptitious manner in which the App Defendants' conducted these intrusions confirms their outrageous nature.

632. As a direct and proximate result of the respective App Defendants' actions, Plaintiffs suffered damages.

633. Defendant Path already admitted that it committed this violation.

Count XVI
Invasion of Privacy (Public Disclosure of Private Facts)
(*Against all App Defendants on Behalf the Opperman Plaintiffs*)

634. Plaintiffs' iDevice mobile address books and the contacts and fields therein are private and are not subjects of legitimate public concern. *United States v. Cotterman*, 709 F.3d 952, __ (9th Cir. Mar 8, 2013) (No. 09-10139)(*en banc*) ("iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives …").

635. As described above, the App Defendants' exposed to the public at large and disseminated Plaintiffs' private mobile address books (and/or material portions thereof) not just to themselves, but to numerous others, too, via the Internet and Wi-Fi.

636. Via their acts, each App Defendant has also divulged and/or disseminated at least some portion of the contents of Plaintiffs' private mobile address books to: (i) wireless and/or cell phone service providers (*e.g.*, AT&T, Sprint and/or Verizon for iPhone users) through which these materials must pass while in transmission over the Internet; (ii) third party server system owners; and/or (iii) their own organizations and their information technology personnel.

637. The App Defendants' public disclosure and dissemination of these Plaintiffs' private

mobile address books – which reveal sensitive information on who the Plaintiffs affiliate, communicate, work and socialize with – is offensive and objectionable to reasonable persons of ordinary sensibilities.

638. Indeed, "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders [an invasion of such interest] more intrusive than with other forms of property." *United States v. Cotterman*, 709 F.3d 952, __ (9th Cir. Mar 8, 2013) (No. 09-10139)(*en banc*).

639. As a consequence of the App Defendants' conduct, this private information was publicly disclosed, and Plaintiffs suffered damages.

640. The App Defendants' conduct was intentional and malicious.

Count XVII
Conversion
(*Against All Defendants on Behalf of All Plaintiffs Except Pirozzi*)

641. Apple unconditionally sold and tendered to Plaintiffs their iDevices. Apple did not condition Plaintiffs' purchase of their iDevices upon any pre-disclosed terms (other than payment). Plaintiffs own their iDevices. Plaintiffs' iDevices are tangible personal property.

642. Plaintiffs own their iDevice mobile address books. Plaintiffs' mobile address books and the materials contained therein are intangible personal property.

643. Apple has acknowledged in its Address Book Programming Guide that Plaintiffs "own" their iDevice mobile address books. The App Defendants have agreed that Plaintiffs own their iDevice mobile address books, too.

644. Plaintiffs' property ownership rights in their iDevices include the right to set terms and compensation for any allowed use of their iDevices. These rights have marketable, economic value. Rent Cell Technologies, Global Advanced Communications, and InTouch USA, for instance, offer daily, weekly and monthly iDevice rental plans with short-term, daily rental rates from $10 to $15 per day in the United States.

645. Plaintiffs' private mobile address books have intrinsic, extrinsic and commercial value. Harris Poll surveys value individuals' mobile address books, like those of the Plaintiffs, at

around $17,000 apiece. Market studies value generic contact lists containing email addresses at approximately $0.60 to $3.00 per contact on a per-contact basis. Companies like Lead 411 solicit and buy individual mobile address books and data aggregators and others routinely buy, sell and license contact lists. Thus, a market has existed for the purchase, sale and exclusive or non-exclusive license of contact information, contacts lists and, more recently, mobile address books.

646. Plaintiffs have superior rights to those that may be claimed by any Defendant with respect to their respective iDevice and mobile address book assets.

647. Plaintiffs' ownership rights in their iDevices and mobile address books include the exclusive right of possession and control. Plaintiffs' ownership rights also include the sole and exclusive right to sell, transfer, license or allow use of their iDevices or their mobile address books and to set terms applicable to any such rights that any Plaintiff chooses to grant.

648. Plaintiffs' property ownership rights in their iDevices and their mobile address books are also superior to any Defendant's right in or to Plaintiffs' iDevices or their mobile address books.

649. Without compensation to and without asking permission from Plaintiffs, the App Defendants and Apple (via the deployed malware and computer contaminants) each exercised dominion and/or control over Plaintiffs' iDevices and mobile address books to the exclusion of, or inconsistent with, Plaintiffs' exclusive rights.

650. Without alerting or seeking permission from Plaintiffs, Apple and the App Defendants also took control of Plaintiffs' iDevices, used iDevice resources, and caused Plaintiffs' iDevices to execute unauthorized commands and trigger unauthorized transmissions, including transmissions that disseminated to the Internet and transferred Plaintiffs' mobile address books to the App Defendants.

651. Without alerting, seeking permission from or compensating Plaintiffs, the App Defendants publicly disseminated Plaintiffs' mobile address books (and/or material portions thereof) over the Internet, sent Plaintiffs' mobile address books to unintended and unauthorized recipients (including themselves), obtained Plaintiffs' mobile address books, and used on their

servers and kept Plaintiffs' mobile address books.

652. Inconsistent with Plaintiffs' rights, the App Defendants and Apple by their actions have exercised control over, converted, trespassed upon and deprived Plaintiffs of the intrinsic, extrinsic and commercial sale and use/rental/licensing value of their iDevices and mobile address books.

653. The App Defendants, with Apple's approval, assistance and participation, converted and trespassed upon Plaintiffs' valuable personal property, invaded Plaintiffs' privacy and seclusion, and publicly exposed Plaintiffs' protected private information. Without asking or compensating Plaintiffs, they (i) took control of and used Plaintiffs' iDevices for unauthorized purposes, and (ii) exercised dominion over, obtained, invaded, publicly exposed and de-privatized Plaintiffs' private mobile address books.

654. The interferences with Plaintiffs' mobile address books were severe. As a direct and proximate result of Defendants' acts, the fundamental nature and character of Plaintiffs' mobile address books were altered: they lost their Constitutional protections once Defendants disseminated and obtained them.

655. Thus, without seeking permission from Plaintiffs, Apple and the App Defendants converted Plaintiffs' iDevices, mobile address books, and mobile address book contacts for the App Defendants' own use and benefit.

656. The App Defendants' acts were intentional.

657. As a direct and proximate result of the App Defendants' acts, each Plaintiff has sustained recoverable damages for the conversion by Apple and each respective App Defendant of his or her iDevice and/or mobile address book (or portions thereof).

658. Plaintiffs each had more than one hundred contacts in their iDevice mobile address books at all relevant times.

659. Plaintiffs are each entitled to recover for conversion from Apple and each respective App Defendant that exercised control over his or her iDevice or mobile address book, (i) the original purchase or the highest fair present value of their iDevice, and (ii) the fair value of their

mobile address books, whether valued in the aggregate ($17,000 based on Harris Poll surveys) or on a per-contact basis (at no less than $0.60 to $3.00 per contact according to industry reports).

660. Plaintiffs are also entitled to recover any economic or other benefit that Defendants unjustly received or obtained from converting Plaintiffs' iDevices or mobile address books and to have a constructive trust imposed over any benefits or proceeds.

661. Defendants' conduct described herein was willful, malicious and oppressive, and constitutes despicable conduct in conscious disregard of Plaintiffs' rights. Plaintiffs are therefore entitled to punitive and exemplary damages in an amount according to proof.

Count XVIII
Trespass to Personal Property and/or Chattels
(*Against All Defendants on Behalf of the Opperman Plaintiffs*)

662. Plaintiffs' iDevices and mobile address books constitute chattel and personal property.

663. As described, Apple and the App Defendants have each wrongfully, intentionally and without seeking (or obtaining) permission interfered with the respective Plaintiffs' possessory interests in and use of their iDevices and their mobile address books.

664. The Defendants' intermeddling and interference was conducted surreptitiously and without authorization of Plaintiffs.

665. Defendants' unauthorized use and interference with Plaintiffs' iDevices depleted iDevice resources, including battery life, memory, wireless airtime, and energy, and resulted in loss of useful iDevice life.

666. Defendants' unauthorized use and interference with Plaintiffs' iDevices also caused harm to other personal property owned by Plaintiffs – the mobile address books – and Plaintiffs' legally protected interests in them, as they were disseminated, de-privatized and de-valued as a proximate result of these unauthorized iDevice uses.

667. These Defendants' acts impaired the condition, use, value and quality of Plaintiffs' iDevices and their address books and proximately caused Plaintiffs to suffer damages.

668. Defendants' interference with Plaintiffs' mobile address book impaired the

condition, quality and value of Plaintiffs' mobile address books by de-privatizing them and by diminishing or eliminating Plaintiffs' ability to control or inhibit the subsequent disclosure or use of the his or her mobile address book materials by the Defendants.

669. As a direct and proximate result of Apple and the App Defendants' acts, each Plaintiff has sustained recoverable damages for the trespass to his or her iDevice and mobile address book.

670. Plaintiffs are each entitled to recover from Apple and each respective App Defendant (i) the higher of (a) a $10 minimum daily market rental rate for each day in which an App Defendant's identified App exercised unauthorized control over and used a Plaintiff's iDevice or caused it to execute an unauthorized address book transmission, or (b) the economic value all iDevices resources depleted by Defendants' action, including battery life, memory, wireless airtime, and energy and all resulting loss in useful iDevice life, and (ii) the highest reasonable unrestricted, worldwide mobile address book use or licensing fee – calculated either as a reasonable percentage (from 5% - 20% as determined by a jury) of that asset's value ($17,000 based on Harris Poll surveys) or on a per-contact basis (at no less than $0.60 to $3.00 per contact according to industry reports) – from each App Defendant who obtained, retained or used that Plaintiff's mobile address book or portions thereof and from Apple who helped them do so).

671. Put more simply, these defendants owe Plaintiffs a customary market rental fee for using their iDevices and a license or use fee for obtaining and using (or having the ability to use) their mobile address books.

Count XIX
Violations of the Texas Theft Liability Act,
TEX. CIV. P & REM CODE § 134.001/TEX. PEN. CODE § 31.03
(Against All App Defendants on Behalf of the Texas Plaintiffs)

672. Plaintiff's iDevices are "property" under TEX. PENAL CODE § 31.01(5)(b). Plaintiffs' personal mobile address books, and their data therein, whether in electronic or physical media, is also "property" under TEX. PENAL CODE § 31.01(5). Plaintiffs own their respective iDevices and their personal mobile address books maintained on their iDevices

673. By their actions described herein, the App Defendants have unlawfully appropriated

each Plaintiff's iDevice and at least a portion of their iDevice mobile address book within the meaning of TEX. PENAL CODE §§ 31.01(4) and 31.03(b)(1). The non-consensual taking of Plaintiffs' mobile address books and the transmission to the App Defendants constitutes a "transfer [of a] . . . non-possessory interest in the [user's mobile address book] to" the App Defendant, consumes device processing power, battery power and life, band-width, electricity and wireless and cellular airtime during the surreptitious transmissions, and causes the unauthorized disclosure and de-privatization of those materials. Plaintiffs did not effectively consent to these actions

674. Incident to the non-consensual transmission and uploading of their mobile address books, Plaintiffs were deprived of airtime on their iDevices and computing and processing power, resources and battery life. Plaintiffs also were deprived of control over their mobile address book materials and of the data's value. Defendants have de-privatized the data and it is unlikely that any defendant will be readily able or willing return or fully expunge from their computer systems and social networks the data, nodes and connections created therein based upon the Plaintiffs' appropriated mobile address book materials

675. Accordingly, each App Defendant has committed theft under TEX. PENAL CODE § 31.03 against each Texas-based Plaintiff and Class Member. On information and belief, the aggregate value of all address book materials acquired by each App Defendant is, in the aggregate, substantial and in excess of $200,000. Because each App Defendant's thefts are part of one scheme, the amounts also may be aggregated for violations under TEX. PENAL CODE § 31.03(e)(7).

676. Plaintiffs had a possessory interest in their identified property, which was unlawfully appropriated from them by each App Defendant.

677. Each App Defendant is consequently liable to each Texas-based Plaintiff and Class Member under TEX. CIV. PRAC. & REM. CODE § 134.03.

678. The Texas-based Plaintiffs and Class Members sustained damages as a result of the App Defendants' actions and are entitled to recover from them actual damages for each theft. *See* TEX. CIV. PRAC. & REM. CODE § 134.04. On information and belief, the actual damages should be no less than the fair market value to acquire in an arms-length transaction the property appropriated

(i.e., the market value of the appropriated mobile address book materials), as set out above.

679. Under Texas' Theft Liability Act, each Texas-based Plaintiff and Class Member is also entitled to recover from each App Defendant who has stolen any portion of the mobile address book from his of her respective iDevice(s) an additional sum as determined by the trier of fact of up to $1,000 per each separate instance of theft.

Count XX
Common Law Misappropriation
(*Against All App Defendants on Behalf of the Opperman Plaintiffs*)

680. The App Defendants intentionally and willfully appropriated material of each Plaintiff's private mobile address books.

681. Plaintiffs expended substantial time and effort collecting the contacts in, and over time assembling, their mobile address books.

682. Each App Defendant has (via its respective Apps) automatically, secretly, and with little effort harvested and/or swept into their computers systems and social and data networks some or all of the fields from Plaintiffs' private mobile address books and used those materials at their own discretion, for their own purposes and to their own benefit.

683. Thus, the App Defendants have impermissibly mined their App users' iDevices for contacts data, thereby obtaining an unjustified and inequitable free ride on and benefit from Plaintiffs' prior efforts

684. As a direct and proximate result, Plaintiffs have suffered damages.

Count XXI
Strict Products Liability – Design Defect
(*Against Apple on Behalf of the Opperman Plaintiffs*)

685. Plaintiffs incorporate by reference all the foregoing allegations as though set forth herein.

686. Apple manufactured and sold the iDevices to Plaintiffs.

687. Plaintiffs used their iDevices as intended and in manners reasonably foreseeable by Apple to (i) maintain their private mobile address books, and (ii) add Apple-issued apps to their

iDevices, including Defendants' Apps. Both uses are purposes for which Apple designed the iDevice products.

688. Apple iDevices were defectively designed by Apple. In part, they did not keep the Contacts database (or Plaintiffs' mobile address books maintained therein) secure.

689. The iDevice did not perform as safely as an ordinary consumer would have expected it to perform when used or misused in an intended or reasonably foreseeable way.

690. The iDevice's failure to perform safely was a substantial factor in causing these Plaintiffs' harm.

691. The benefits of Apple's chosen design do not outweigh the risk of danger inherent in such design.

692. The design violated minimum industry and Apple-promised safety standards.

693. Plaintiffs were harmed when using the iDevices in their intended way.

694. As a proximate cause of these defective designs, Plaintiffs were harmed and damaged as described above. Notably, Plaintiffs suffered personal injuries as a result of the defective design, including invasions of their privacy and damages to their properties (the mobile address books).

695. Plaintiffs suffered damages and personal injuries as described herein (including the invasion of their privacy and conversion of their mobile address books) as a proximate result of Apple's defective and/or negligent design of the iDevices, the failure of those iDevices to comply with Apple's express pre-purchase warranties and promises, and Apple's failure to adequately warn Plaintiffs about iDevices' susceptibility to mobile address book harvesting and its App Store-listed apps that contained those functions.

696. Apple could have, but chose not to, employ any one of a number of inexpensive techniques to adequately secure iDevices and their contacts databases and eliminate iDevice and their contacts database susceptibility to privacy-invading mobile address book harvesting functions like those employed in the identified apps

697. Apple is strictly liable to Plaintiffs.

Count XXII
Strict Product Liability – Failure to Warn
(*Against Apple on Behalf of the Opperman Plaintiffs*)

698. Apple iDevices lacked sufficient or adequate warnings of potential adverse risks, including dangers to users' privacy and to the property (mobile address books) that they maintain with those iDevices.

699. iDevices had potential risks that were known or reasonably knowable to Apple in light of the technology and information available to it. Specifically, as known to Apple but not to ordinary users, iDevices did not "sandbox" the Contacts database for security and privacy purposes to prevent its access, alteration or transmission by other Apps, which left the Contacts database and user's private mobile address books maintained therein) exposed to those precise risks: an alteration, taking or exposure.

700. This potential risk presented a substantial danger to users, like these Plaintiffs, when they used the iDevice (or misused it) in an intended or reasonably foreseeable way, such as to maintain their private mobile address book and contacts and to add various aftermarket Apps to the iDevice.

701. Ordinary consumers like the Plaintiffs would not have recognized this potential risk.

702. Apple failed to adequately warn or instruct Plaintiffs of these potential risks or how to appropriately avoid them.

703. As a result, Plaintiffs were harmed. Their personal property was relayed and disclosed to others.

704. The lack of sufficient instructions and/or warnings was a substantial factor in causing Plaintiffs' harm.

705. Apple is strictly liable to Plaintiffs.

XXIII
Negligence
(*Against All Defendants on Behalf of All Plaintiffs Except Pirozzi*)[33]

[33] Plaintiffs Arabian and Carter bring claims under this Count against Defendants Instagram and Path, respectively, and do not assert claims under this Count against Defendant Apple.

706. The App Defendants intentionally and willfully appropriated, either in whole or in part, bulk portions of each Plaintiff's iDevice's private address books.

As to the App Defendants

707. App Defendants violated criminal law and general standards of care by putting out malware that invades user privacy. App Defendants owed a duty to Plaintiffs and Class Members to protect their personal information and data property and take reasonable steps to protect them from the wrongful taking of such information and the wrongful invasion of their privacy.

708. This duty was not based on any contractual obligation but arose, instead, as a matter of law because, at all times, App Defendants knew or should have known of the likelihood of harm arising from Defendants' failure to act reasonably under the circumstances alleged herein.

709. App Defendants had an obligation to use reasonable care to prevent such harm or to adequately warn Plaintiffs and Class Members of such harm.

710. App Defendants breached the duty of care owed to Plaintiffs and Class Members by, among other things:

i) Accessing and storing Plaintiffs' and Class Members' personal information and transmitting such information to third parties, without Plaintiffs' and Class Members' knowledge or consent;

ii) Transmitting Plaintiffs' and Class Members' personal information in an unreasonably insecure manner—contrary to accepted standards; and

iii) Using Plaintiffs' and Class Members' personal information for their own unrelated purposes without Plaintiffs' and Class Members' knowledge or consent.

711. As a direct and proximate result of App Defendants' breaches of their duties, Plaintiffs and Class Members suffered the harm described more fully above, each of which were a reasonably foreseeable result of App Defendants' negligence.

As to Apple

712. Apple was negligent as it:

- Failed to conduct rigorous reviews as promised;
- Failed to protect Plaintiffs' and consumers' privacy, particularly with regard to their address books, as promised;
- Failed to warn Plaintiffs and consumers about malicious Apps it distributed and known iDevice security risks;
- Failed to correct multiple misrepresentation concerning privacy protection and iDevice security.
- Failed to meet common industry standards relating to iDevice privacy and security and design.

713. As a direct and proximate result, Plaintiffs suffered damages to their person and property.

714. Plaintiffs' damages include, *inter alia*, reasonable expenses for each Plaintiff to remedy and prevent the security breaches exposed by the App Defendants' wrongful conduct, recoupment of the value of the address books appropriated from their iDevices and the de-privatization of those materials, and other economic and noneconomic harm—for which they are entitled to compensation.

715. Defendants' wrongful actions and/or inaction (as described above) constitute negligence at common law, negligence *per se*, negligence and gross negligence.

Count XXIV
Violation of the Uniform Fraudulent Transfer Act
(*Against Gowalla and Facebook on Behalf of the Gowalla Plaintiffs*)

716. *Gowalla*, Facebook, *Gowalla*'s management personnel and *Gowalla*'s owners entered into a transaction in violation of California's Uniform Fraudulent Transfer Act, Cal. Civ. Code § 3439 (the "Act"), as described above.

717. *Gowalla* was insolvent or on the verge of insolvency at the time it entered into the described transaction.

718. *Gowalla* did not receive fair value in exchange for that transaction.

719. The transaction left *Gowalla* without the means, ability or resources to satisfy creditor claims.

720. Facebook, *Gowalla* and its owners and managers structured and carried out that transaction knowing that *Gowalla* would not receive fair value in exchange for that transaction, would be left insolvent and lacking continuity, that payments would be redirected to *Gowalla* owners and management and that creditor claims could not be satisfied as a result of that transaction.

721. Plaintiffs are creditors within the meaning of the Act and harm been harmed.

722. Plaintiffs are entitled to exercise all rights allowed by under the Act and by law to satisfy their claims, including avoidance of the transaction, immediate attachment of the transferred assets or proceeds thereof (wherever and with whomever they may reside), and immediate appointment of a receiver.

Count XXV
Violations of R.I.C.O., 18 U.S.C. §§ 1961-1964
(*Against All Defendants on Behalf of the Opperman Plaintiffs*)

723. Plaintiffs re-allege the previous paragraphs.

724. Apple and these App Defendants engaged in an ongoing, multi-year malware distribution ring which facilitated and allowed the App Defendants to surreptitiously and unlawfully appropriate and obtain for themselves the valuable private mobile address books of millions of iDevice owners.[34] Chillingo, ZeptoLab and Rovio also conspired with one another to form a satellite malware creation and distribution ring to accomplish the same object.

725. Defendants' identified Apps did not request permission to transmit or disclose iDevice owners' private mobile address book materials to third parties before instructing iDevices to silently do so.

726. Each App Defendant intentionally designed and built its App to operate this way. The identified Apps were pre-programmed to trigger iDevices to relay iDevice owners' private

[34] For clarification, each App Defendant is presently alleged to have independently conspired with Apple, who sequentially added to the App Store and deployed roughly a dozen different types of malware to millions of consumers' iDevices.

mobile address books to the App Defendants' server. Each App lacked visible, explicit on-device alerts requesting prior user consent to do so. No App cryptographically hashed or anonymized the content of the mobile address book before it was transmitted.

727. As a direct, proximate and intended result, each App Defendant surreptitiously obtained Plaintiffs' and the Class members' valuable property (their mobile address books or substantial portions thereof) by the remote unauthorized control and use of Plaintiffs' and the Class members' iDevices. Each App Defendant thus obtained tens of thousands to millions of iDevice owners' valuable private mobile address books, amounting in the aggregate to billions of unique contacts.

728. As a proximate consequence of the unauthorized App-initiated iDevice transmissions, iDevice owners' private mobile address book materials were also publicly disclosed to innumerable persons via Wi-Fi, 3G, wireless and the Internet.

729. Apple helped each App Defendant design, build, market, sell, deploy, install and active on owners' iDevices each of their Apps through the App Store Sales Channel and the iOS App Developer Program.

730. Apple set up and managed the networked on-device App Store, the cloud-based App Store store, and the overall digital customer sales and marketing channel as a sales outlet for iDevice Apps. The cloud-based App Store servers on which Apple loads and stores available Apps may be owned by Apple. Nevertheless, the overall networked App Store customer sales channel (the "Sales Channel") is not. It is extraneous to Apple; Apple and each iDevice owner (of which there are hundreds of millions) are members in that network. iDevice owners associate through the networked App Store Sales Channel with Apple and with one another via their tethered and networked iDevices to view, communicate about, rate and obtain iDevice Apps offered by Apple. It is an association of members and forms an enterprise.

731. The App Store Sales Channel, which is managed from California, affects and is involved in interstate commerce. For instance, consumers and businesses from all fifty states and abroad regularly communicate through the App Store Sales Channel both wirelessly and over the

Internet. Apple, through the cloud-based App Store also regularly post Apps received from all over the world to the cloud-based App Store store and, when purchased, transmits those Apps all over the world to persons in all fifty states and abroad, both wirelessly and via the Internet, over the App Store Sales Channel to networked iDevices.

732. Each App Defendant has communicated with or through the App Store Sales Channel (including via online and on-device App Store marketing of their apps), associated with Apple through the App Store Sales Channel, and listed their Apps on the cloud-based App Store store and deployed their Apps to consumers through the networked App Store Sales Channel.

733. The App Store Sales Channel is an enterprise. The App Store Sales Channel has a continuous, ongoing, hierarchical and ascertainable structure, which has been in place since at last mid-2008. Structurally, the App Store Sales Channel is a closed, client-server product marketing, deployment and sales channel network. The App Store Sales Channel forms a relational structure between Apple, each of the App Defendants and all other developers of Apple-approved Apps, and millions of owners of networked, tethered iDevices. Apple and each App Defendant associated and worked together through the networked App Store Sales Channel enterprise for the purposes of listing, promoting and wirelessly deploying Apps to consumers' iDevices and, ultimately, to make money and increase their product adoption and user bases.

734. Apple also set up and managed the networked iOS App Developer Program ("Program") so that developers, including the App Defendants, could associate, work and communicate with Apple and one another and share resources and know-how to design, build and release Apps for iDevices.

735. In fact, only Program members can use Apple's development tools, code, and application programming interfaces ("APIs"), access the retail side of the App Store Sales Channel, and communicate with and wirelessly deploy apps on the expansive consumer network of iDevices tethered to Apple's networked, cloud-based App Store store.

736. Within the Program, Apple and all App Defendants acknowledged Plaintiffs' and other Class members' ownership of their respective mobile address books in contractual Program policies and procedures mandated upon Apple and the App Defendants by Apple.

737. The Program is run from California and affects and is involved in interstate commerce. For instance, businesses and individuals from all fifty states and internationally regularly communicate through and with the Program via the Internet. Apple, via the Program, also regularly receives via the Internet apps submitted from around the world.

738. Each App Defendant has communicated with or through the Program, associated with Apple through the Program, and submitted its Apps to Apple through the Program.

739. The Program is an enterprise. The Program has a continuous, ongoing, hierarchical and ascertainable structure, which has been in place since mid-2008. Structurally, the Program is a networked association of Apple and its Program-registrant App product developers. The Program forms a relational structure between Apple and each of the Program registrants (i.e., app developers), including each of these App Defendants. (Literally, they are associated members in a Program led by Apple). Apple and each of the Program registrants (including each of the App Defendants) associated through the Program enterprise for the purposes of building and releasing apps for consumers' iDevices and, ultimately, to make money and increase their product adoption and user bases.

740. As described above, Apple and each App Defendant represented to Plaintiffs, Class members and the public at large that Apps from the App Store, including their Apps in particular, would not contain malware or functions (like those described above) that result in others' non-consensual acquisition of the iDevice owners' private data or property. Apple and each App Defendant repeatedly made those representations, in part, to encourage Plaintiffs, Class members and other consumers to obtain and accept Apps (including theirs) from the App Store. In view of the information within their knowledge and possession, Apple and each App Defendant knew its representations were not true or were reckless as to their truth or falsity when made.

741. The App Defendants' identified Apps are malware under common industry definitions and Apple's own definitions cited herein.

742. Apple regularly assured customers and, via its FCC Letter, the federal government that it thoroughly tests, reviews and knows the content, features and functions of each iDevice App before adding it to the cloud-based App Store store or deploying it to and activating it on consumers' iDevices.

743. Apple reviewed and tested the App Defendants' identified Apps, and, accordingly, knew their contents, features and functions. Apple was thus aware that each identified App, when operated as intended, could and would trigger an iDevice transmission of the iDevice owner's private mobile address books to the App Defendants' server but lacked an in-advance, visible, explicit, on-device alert requesting prior user consent to do so. Apple thus knew that the App Defendants' identified Apps were malware under its own and other common industry definitions and that these Apps did not comply with various Program standards.

744. Despite assurances to Plaintiffs and millions of Class members, Apple and the App Defendants nevertheless released these Apps to the cloud-based App Store store and, through the App Store Sales Channel, marketed and nonetheless deployed these malware Apps to Plaintiffs and millions of other Class members' iDevices. As between Apple and each App Defendant (but unknown to consumers), Apple served and operated as each App Defendants' agent for these activities and shared in revenues related to the Apps.

745. Thus, despite express promises by all not to do so, Apple and each App Defendant thus also worked together and used the Program and the Sales Channel enterprises to knowingly, collaboratively, intentionally and repeatedly create then deploy illegal computer-contaminating malware (the identified Apps) on Plaintiffs' and millions of Class members' iDevices, which then took control of those iDevices as described above and relayed the Plaintiffs' and the Class members' valuable private mobile address books to the respective App Defendants via the Internet.

746. These unauthorized transmissions relayed the Plaintiffs' stolen mobile address books across state lines and through interstate commerce over the wires.

747. The App Defendants thus obtained and damaged Plaintiffs' and millions of Class Members' valuable private mobile address books and used their iDevices in unauthorized manners in disregard of Plaintiffs' property and privacy rights and without compensation to Plaintiffs.

748. This conduct occurred over the course of several years.

749. Apple and each App Defendant benefited as a result of this conduct and are continuing to retain the benefits from that wrongful conduct.

750. Apple and each App Defendant thus committed RICO violations by conspiring to commit racketeering activities, including infecting iDevices with malware via the Internet (wire fraud) and thereby stealing and transporting mobile address book properties across state lines (transportation of stolen property), in repeated violations of the RICO Act.

751. Apple and each App Defendant is a "person" under the RICO Act.

752. The App Store Sales Channel and the Program each constitute an "enterprise" under the RICO Act.

753. Apple operates, manages and participates in both the Program and the App Store Sales Channel. Each App Defendant associates with Apple through both the App Store Sales Channel and the Program (in which they are all registered members).

754. The App Store Sales Channel and the Program both have organized, networked, hierarchical and ongoing structures and affect interstate commerce. The ordinary ongoing purpose for the App Store Sales Channel and the Program is for Apple and its Program participants, including each App Defendant, to build, release, sell and deploy legal and compliant Apps to consumers' iDevices and, ultimately, increase sales, expand customer bases and make money.

755. Apple and each App Defendant have nevertheless conspired to engage in patterns of racketeering activity through the App Store Sale Channel and the Program enterprises.

756. Specifically, they have used the Program and the App Store Sales Channel to knowingly create and repeatedly place malware, computer contaminants and non-compliant Apps on the iDevices of the Plaintiffs' and myriad other Class members and thereby steal and transport from those same persons' iDevices valuable property: their private mobile address books.

757. As discussed above, these racketeering activities continued over a period of several years.

758. As a consequence, Plaintiffs and the Class members were damaged in their business and/or their property. For instance, their iDevices were infected with malware and used in unauthorized manners to further injure Plaintiffs, their property and their privacy by disclosing, disseminating and transferring to others, including the App Defendants, Plaintiffs' valuable private mobile address books.

759. To date, Apple and the App Defendants are continuing to conceal their conduct from the Plaintiffs and to retain the benefits of their wrongful conduct. For instance, they still have not individually informed any iDevice owners about the appropriation of their mobile address books.

760. **Wire Fraud (18 U.S.C. § 1343)**

761. Violations of 18 U.S.C. §§ 1343 (wire fraud) and 2314 (transportation of stolen property) are predicate acts under the Racketeering Influence & Corrupt Organizations Act (18 U.S.C. § 1962, et seq.). 18 U.S.C. §§ 1961(1).

762. Defendants' placement of malware and computer contaminants on Plaintiffs' and millions of Class members' iDevices to obtain their property constitutes wire fraud.

763. The Defendants persuaded Plaintiffs and the Class members to accept the malware and computer contaminants under false pretenses. They were told that apps from the App Store would not contain malicious or privacy-invading functions, that their iDevices were sandboxed and consequently should not be susceptible to address-book harvesting, that Apple and these App Defendants complied with laws and their Apps respected users' privacy. (Plus, computer contaminants are nevertheless illegal and prohibited.)

764. As discussed above, these statements were false.

765. These communications and the malware were sent via the wires.

766. Apple and each App Developer jointly promoted and deployed on Plaintiffs' and others' iDevices and knew the content of each App Defendant's respective App.

767. Apple even privately encouraged the App Defendants to create Apps having these malicious features[35] despite publicly touting otherwise, stating "don't force people to give you information you can easily find for yourself, such as their contacts or calendar information"

768. The focal object of the Defendants' scheme was to surreptitiously and without permission obtain iDevices owners' property, specifically, their mobile address books, for their business purposes. Apple and each App Defendant had a common purpose and meeting of the minds to deploy each respective App Defendant's malicious App on Plaintiffs' and other Class members' iDevices.

769. The Defendants were successful. As discussed above, the Plaintiffs' and others' mobile address books were transmitted and relayed to the App Defendants. These transmissions also occurred via the wires.

770. Thus, Apple and each App Defendant employed false pretenses so that Plaintiffs and others would accept the App Defendants' Apps on their iDevices. The App Defendants thereby wrongfully and as part of a scheme to defraud obtained Plaintiffs' mobile address books or material portions thereof.

771. Apple'sknowing issuance of false public statements and advertisements also helped further this scheme.

772. Apple and each App Developer each caused bulk portions of the Plaintiffs' private mobile address books to be transmitted as electronic signals in interstate commerce by means of wires and the airwaves for the purposes of and in furtherance of executing these schemes. The transmission of Plaintiffs' and others' mobile address book from the iDevices via the wires constitutes a secondary instance of wire fraud.

[35] Apple's *Human Interface Guidelines*, excerpt available on Apple's website at http://developer.apple.com/library/ios/#documentation/UserExperience/Conceptual/MobileHIG/TechnologyUsage/TechnologyUsage.html#//apple_ref/doc/uid/TP40006556-CH18-SW1 and http://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/MobileHIG/MobileHIG.pdf .

773. Accordingly, Apple's and each App Defendants' described actions constitute a conspiracy to commit wire fraud under 18 U.S.C. § 1343.

774. **Transportation of Stolen Property (18 U.S.C. § 2314 cl.2):**

775. With Apple's participation and assistance, each App Defendant obtained Plaintiffs' and the Class members' property (material portions of their mobile address books) by means of false pretenses under a scheme to defraud. In the aggregate, the value of the property each App Defendant wrongfully obtained exceeds $5,000.

776. Each App Defendant transported material portions of the appropriated mobile address books and/or caused those portions to be transported in interstate commerce and across state lines (by, for example, relaying it from iDevices over computer and wireless networks, including the Internet) in furtherance of their schemes.

777. Hence, Defendants have participated in rings that traffic in, make use of, and benefit from private mobile address book materials obtained from Plaintiffs' and Class members' iDevices.

778. Defendants' actions constitute transportation of stolen property in violation of 18 U.S.C. § 2314.

779. Each App Defendant and Apple jointly and collaboratively committed thousands of predicate acts of wire fraud and each App Defendant with Apple's assistance committed thousands of predicate acts of transportation of stolen property.

780. **Racketeering Influence & Corrupt Organizations (18 U.S.C. § 1962)**

781. The App Defendants' wire-tapping activities and transportation of stolen property was facilitated by and committed with the knowing assistance, encouragement and participation of Apple in contravention of Apple's own standards, policies, agreements, procedures and representations to the consumer market.

782. Each App Defendant in conjunction with Apple conducted or participated in the conduct of the affairs of an enterprise engaged in interstate commerce through a continuous pattern of racketeering activity – here, numerous repeated instances of wire-tapping and transportation of

stolen property (not to mention criminal violations under the CCL and ECPA) over several years – in violation of 18 U.S.C. § 1962(c).

783. Each of the App Defendants, in conjunction with Apple, have formed, associated and participated in an enterprise or association via the App Store Sales Channel and the Program.

784. Moreover, the defendants have pursued the common purpose of making money, gaining market-share, adding persons, nodes and cross-links into their social networks, and expanding their networked databases illegally via the promotion and sale in interstate commerce of the offending Apps that automatically and without informing users surreptitiously uploaded and made use of owners' iDevices and that intercepted and took owners' mobile address books. (The Defendants have associated and used the App Store Sales Channel enterprise to send malware to millions of consumers' iDevice and turns them into zombie bots.) This association exists separate and apart from the pattern of racketeering being pursued by these defendants.

785. The defendants have in combination and collaboration pursued the common purpose of illegally profiting upon, via the development, promotion, sale and deployment in interstate commerce of malware (the distributed Apps) that automatically and surreptitiously invaded iDevice owners' privacy, triggered breaches of users' computer security, and stealthily and automatically committed unauthorized disclosures and transmissions in interstate commerce of iDevice owners' private mobile address book data in violation of federal and state statutes.

786. They combined and conspired to promote and intentionally deploy onto Plaintiffs' and Class members' iDevices via the wires harmful malware containing known computer contaminants designed to take control of and steal owners' property – the mobile address books – despite express promises by all not to do so.

787. Apple and each App Defendant conducted or participated in the conduct of the affairs of an enterprise engaged in interstate commerce through a pattern of racketeering activity – in violation of 18 U.S.C. § 1962(c) – here, numerous repeated instances of wire fraud and transportation of stolen property harmful to the Plaintiff, the Class members, and the public.

788. Apple and the identified App Defendants combined to engage in patterns of racketeering activity in violation of 18 U.S.C. § 1962(d) and engaged in unconscionable, unfair or deceptive practices in or affecting commerce in violation of 15 U.S.C. § 45 that knowingly facilitated and resulted in a stream of technologically-harmful App products coming to market that turn an owner's otherwise functional iDevice into an eavesdropping device that without permission surreptitiously transmits and broadcasts to others the iDevice owner's private mobile address books. The Defendants directly and indirectly receive income and benefits from these patterns of activities.

789. Each App Defendant and Apple directed and controlled the illegal conduct described herein and Apple was involved in and directed and controlled the management of the enterprises themselves – the App Store and the Program.

790. Plaintiffs have been directly harmed in their business or their property (i.e., their private mobile address books and iDevices) as described herein a result of these Defendants' violations of 18 U.S.C. § 1962. Accordingly, Plaintiffs are entitled to recover treble damages and attorneys' fees under 18 U.S.C. § 1964.

791. On information and belief, the Defendants' conduct has been intentional and willful in nature.

792. These collaborative actions and schemes constitute wire fraud under 18 U.S.C. § 1343, transportation of stolen property under 18 U.S.C. § 2314, and consequently violate R.I.C.O., 18 U.S.C. § 1961 *et seq.*

793. Apple and the App Defendants have been engaged in a multi-year pattern of racketeering in violation of 18 U.S.C. §§ 1961-1964.

794. In addition to participating in the described overall racketeering conduct, Chillingo has also separately conspired with ZeptoLab and with Rovio to accomplish the same objective through Chillingo's Gaming Platform and Rovio and ZeptoLab's respective Apps.

795. Chillingo operates a program oriented toward gaming apps and their developers (the "Gaming Program"). To participate in the Gaming Program, app developers must register with Chillingo, who operates and manages the Program.

796. Chillingo's Gaming Program helps registrants build apps and also enables registrants to integrate or incorporate Chillingo's *Crystal* into their apps.

797. Rovio and Zepto were both registrants in the Gaming Program.

798. In use, Chillingo's *Crystal* creates a networked leaderboard structure of iDevice owners operated by Chillingo for those registrant apps and their users.

799. The Gaming Program affects and is involved in interstate commerce. For instance, businesses and individuals from all fifty states and internationally regularly communicate through and with the Gaming Program via the Internet. Chillingo, via the Program, regularly integrates *Crystal* via the Internet into Apps from around the world.

800. Rovio and ZeptoLab have communicated with or through the Gaming Program, associated with Chillingo through the Gaming Program, and had *Crystal* integrated into their Apps through the Gaming Program.

801. The Gaming Program is an enterprise. The Gaming Program has a continuous, ongoing, hierarchical and ascertainable structure. Structurally, the Gaming Program is a networked association of Chillingo and its registrants. The Gaming Program forms a relational structure between Chillingo and each of the Gaming Program registrants, including each of these Rovio and ZeptoLab. (They are associated members in a Gaming Program led by Chillingo). Chillingo and each of the Gaming Program registrants (including Rovio and ZeptoLab) associated through the Gaming Program enterprise for the purposes of building and releasing *Crystal*-integrated apps for consumers' iDevices through the App Store Sales Channel and, ultimately, to make money and increase their product adoption and user bases.

802. Chillingo and Rovio and ZeptoLab, also worked together and used the Gaming Program, the networked *Crystal* leaderboard structure, the App Store Sales Channel and the Program to knowingly, collaboratively and repeatedly to create under the Program and the Gaming Program then deploy via the App Store Sales Channel malware (their identified Apps) containing illegal computer contaminants on Plaintiffs' and other Class members' iDevices, which took control

of those iDevices and relayed the Plaintiffs' and millions of Class members' mobile address book properties to Chillingo, Rovio and/or ZeptoLab, via the Internet.

803. Chillingo, Rovio and ZeptoLab were each aware that their apps were designed to, and were, uploading portions of iDevice owners' mobile address books to Chillingo's or Rovio's or ZeptoLab's servers. Each was also aware that explicit permission had not been requested to do so. Each also benefitted as a result of that conduct and have retained the benefits of that conduct.

804. Chillingo, Rovio and ZeptoLab each committed wire fraud, transported stolen property in interstate commerce, and committed RICO violations, as above, by then issuing their *Crystal*-integrated Apps via the App Store Sales Channel.

805.

Count XXVI
Secondary and Vicarious Liability
(*Against All Defendants on Behalf of the Opperman Plaintiffs*)

Vicarious Liability (Apple as App Defendants' Agent)

806. Each App Defendant retained Apple as its agent on matters pertaining to its App, including on marking, listing, deploying and installing the App.

807. Apple served and acted within the scope of the granted authority.

808. Each App Defendant is vicariously liable for acts committed and harmed caused by Apple while acting within the scope of its agency for that App Defendant.

Aiding And Abetting/Assisting And Encouraging (As To Apple)

809. Apple receives substantial financial, economic, advertising, public relations and other benefits from its approval, release, sale and deployment of the identified Apps.

810. Apple materially supported, assisted and helped build, market and deploy the identified Apps and knowingly and/or recklessly permitted the surreptitious collection of Plaintiffs' private mobile address books and unauthorized operations of their iDevice.

811. Before February of 2012, Apple never individually instructed any App Defendant to design its App to hash any bulk uploads of iDevice owners' private mobile address books or to include any address book-related user alerts or permission dialogue boxes in any of their Apps.

812. Apple's encouragement, assistance and support were substantial factors leading to each App Defendant inflicting the above-described injuries and harms on Plaintiffs and a proximate cause of Plaintiffs' damages.

Aiding And Abetting/Assisting And Encouraging as to Facebook

813. On information and belief, Facebook authorized, approved and facilitated the continued distribution of the Gowalla App from late 2011 through March 2012. On information and belief, Facebook provided material support and assistance and helped in the continued production and distribution of the Gowalla App during that period. On information and belief, Facebook conducted due diligence regarding the operation and functionality of the Gowalla App and was aware of the Gowalla App's automated, non-consensual mobile address book data harvesting functionality.

814. Accordingly, for the periods described, Facebook may be both independently and/or jointly and severally liable to the Plaintiffs on each of the claims and for all of the harm and damages described herein pertaining to Gowalla during those periods.

815. , data nodes and coupled data links originally taken or gleaned from Plaintiffs' surreptitiously obtained mobile address book materials.

816. Defendants benefited from the above-described wrongful acts. On information and belief, the App Defendants' acquisition and use of Plaintiffs' and Class members' address book materials facilitated the growth of each of their respective social networking databases and services or gaming platforms, enhancing the overall economic value of each of their respective organizations and business operations for fundraising, acquisition, advertising and other purposes.

817. The Defendants and Apple have received revenues and other benefits associated with their distribution and/or sales of the non-conforming malicious Apps identified herein.

818. Each Defendant has received as a result of its wrongful acts, directly or indirectly, funds and other valuable benefits which each company was not rightfully or equitably entitled to in an amount to be determined at trial, and has been unjustly enriched thereby.

DEMAND FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of the members of the Class defined herein, as applicable, pray for judgment and relief as follows as appropriate for the above causes of action:

A. An order certifying this case as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. A temporary, preliminary and/or permanent order for injunctive relief enjoining Defendants from pursuing the policies, acts and practices complained of herein including but not limited to the following:

(i) an order prohibiting the distribution or operation of Apps having coding and/or functionalities that can or do cause either: (A) the unhashed or unencrypted upload of any bulk portion of an iDevice owner's address book materials, and (B) the upload of any such address book materials prior to an alert and the owner granting explicit, knowing permission for the upload and any subsequent use of such materials;

(ii) an order prohibiting any continued non-authorized use of Plaintiffs' address book materials and requiring the return and/or deletion from Defendants' computers and computer systems—as verified by an independent third party data security company—of any wrongfully obtained portions of Plaintiffs' address book materials as well as any data, data nodes or data connections derived therefrom;

(iii) an order requiring Defendants to submit to periodic compliance audits by an independent, third-party data security company regarding the privacy and security of iDevice users' address book materials and the handling of any such materials that may come into Defendants' possession, custody or control;

(iv) an order enjoining Defendants' violations of any of the criminal laws cited herein;

(v) an order mandating that Apple: (a) provide iDevice users with a built-in option for the encrypted storage of their address book on their iDevices, and (b) require hashing of any automatic or bulk uploads of user address book materials for purported matching purposes; and,

(vi) an order directing the Defendants to preserve and maintain throughout the course of this proceeding all evidence pertaining to this matter—including computer and electronic records, historical App code, and records relating to attempts to access the iDevice of any Plaintiff or to subsequently upload, copy, use, store, or disseminate any portion of any Plaintiff's address book materials.

(vii) an order requiring Defendants to undertake an informational campaign to inform members of the general public as to the wrongfulness of their practices

C. An award of actual, statutory, treble, presumed, punitive and/or exemplary damages, as appropriate for the particular Causes of Action;

D. Declaratory relief, as appropriate for the particular Causes of Action;

E. An order requiring disgorgement of Defendants' unjust enrichment, wrongful profit or ill-gotten gains by requiring the payment of restitution to Plaintiff and members of the Class, as appropriate for the particular Causes of Action;

F. Imposition of constructive trusts, as appropriate for the particular Causes of Action over any benefits wrongfully received or obtained by the Defendants or proceeds thereof;

G. An order under 11 U.S.C. § 523(a)(6) that Defendants be prohibited from any discharge under 11 U.S.C.. § 727 for injuries caused to Plaintiffs' and the Class members by Defendants' malicious and willful conduct;

H. Appointment of a receiver, as appropriate for the particular Causes of Action;

I. Reasonable attorneys' fees;

J. All related costs of this suit;

K. Pre- and post-judgment interest; and

L. Such other and further relief as the Court may deem just, necessary, or appropriate.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims and issues herein.

Dated: September 3, 2013

Respectfully submitted,

PHILLIPS, ERLEWINE & GIVEN LLP

By: /s/ David M. Given
PHILLIPS, ERLEWINE & GIVEN LLP
David M. Given (CBN 142375)
dmg@phillaw.com
Nicholas A. Carlin (CBN 112532)
nac@phillaw.com
50 California Street, 35th Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911

LAW OFFICES OF CARL F. SCHWENKER
Carl F. Schwenker (TBN 00788374)
cfslaw@swbell.net
The Haehnel Building
1101 East 11th Street
Austin, Texas 78702
Tel: 512-480-8427
Fax: 512-857-1294

EDWARDS LAW
Jeff Edwards (TBN 24014406)
jeff@edwards-law.com
The Haehnel Building
1101 East 11th Street
Austin, Texas 78702
Tel: 512.623.7727
Fax: 512.623.7729

Counsel for Plaintiffs Alan Beuershasen, Giuli Biondi, Steve Dean, Stephanie Dennis-Cooley, Claire Hodgins, Jason Green, Gentry Hoffman, Rachelle King, Nirali Mandaywala, Claire Moses, Judy Paul, Theda Sandiford, Greg Varner (the Opperman *Plaintiffs) in* 13-CV-00453-JST

GARDY & NOTIS, LLP

By: *s/ Jennifer Sarnelli*
Jennifer Sarnelli (242510)
jsarnelli@gardylaw.com
Kira German (*pro hac vice*)
kgerman@gardylaw.com
501 Fifth Avenue, Suite 1408
New York, NY 10017
Tel: 212-905-0509
Fax: 212-905-0508

LAW OFFICES OF MARTIN S. BAKST
Martin S. Bakst (No. 65112)
msb@mbakst.com
15760 Ventura Boulevard
16th Floor
Encino, CA 91436
Tel: 818-981-1400
Fax: 818-981-5550

Counsel for Plaintiff Maria Pirozzi in 12-CV-01529-JST

STRANGE & CARPENTER

By: /s/ Brian R. Strange
BRIAN R. STRANGE
STRANGE & CARPENTER
Brian R. Strange
(Cal. Bar No. 103252)
LACounsel@earthlink.net
12100 Wilshire Boulevard
Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
Fax: 310-826-3210

Counsel for Plaintiff Lauren Carter in 12-CV-01515-JST *and for Plaintiff Haig Arabian in* 12-CV-06550-JST